Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Transformation Concepts and Technologies: DRDC Tiger Team analysis of Transformation implications

Neal Porter,
Jim Kennedy,
Bert Bridgewater,
et al.

DEFENCE R&D CANADA

Technical Report
TR 2004-003
April 2004

Canada

Transformation Concepts and Technologies

DRDC Tiger Team analysis of Transformation implications

Edited by Neal Porter
DRDC Corporate

With Contributions by:

Jim L. Kennedy
DRDC Atlantic

Georges Fournier
DRDC Valcartier

Doug Hales
DRDC ORD

Doug Hanna
DRDC Suffield

Mazda Salmanian
DRDC Ottawa

Peter Tikuisis
DRDC Toronto

Bert Bridgewater
DRDC Ottawa

Daniel Charlebois
DRDC ORD

Paul D'Agostino
DRDC Suffield

Mark Hazen
DRDC Atlantic

Justin Hollands
DRDC Toronto

Pierre Lavoie
DRDC Ottawa

Dennis Nandlall
DRDC Valcartier

Defence R&D Canada

Technical Report

DRDC TR 2004-003

2004-04-27

104-07452/

Author

Neal Porter, Jim Kennedy, PhD, Bert Bridgewater, PhD, et al.

Approved by

Ingar Moen, PhD
Director of Science and Technology Policy

Approved for release by

Ingar Moen, PhD
Chair, Document Review Panel

© Her Majesty the Queen as represented by the Minister of National Defence, 2004

© Sa majesté la reine, représentée par le ministre de la Défense nationale, 2004

Abstract

The Department of National Defence and the Canadian Forces are presently analysing the implications of Transformation and the future defence and security environment. Defence Research and Development Canada (DRDC) established two Tiger Teams in order to inform and enable that process. The teams conducted a workshop in October 2003 and then exchanged information through the use of a portal before consolidating their findings. One team analysed a variety of Transformation concepts and came to the conclusion that three influences pervaded all of the concepts. These were the issues of the role of culture, the soldier's capability, and being networked enabled. It was felt that DRDC was only very well positioned to support the latter. The other team examined technologies that would enable Transformation in the next 30 years. It determined that directed energy systems and platforms, cyber-war technologies, new materials, and cognitive sciences would be among the disruptive technologies in the future. These are new or existing technologies used in an innovative fashion that will significantly alter established practices. The teams' findings set the stage for further discussion of Transformation and the future science and technology environment.

Résumé

Le ministère de la Défense nationale et les Forces canadiennes sont en train d'analyser l'incidence de la transformation ainsi que le futur cadre de défense et de sécurité. Recherche et développement pour la défense Canada (RDDC) a constitué deux équipes spéciales chargées de la diffusion d'information et de la mise en oeuvre de ce processus. Avant de rassembler leurs constatations, elles ont tenu un atelier, en octobre 2003, puis échangé des renseignements grâce à l'utilisation d'un portail. Une équipe a analysé divers concepts de transformation et en est venue à la conclusion que trois facteurs déterminants se retrouvaient dans tous les concepts. Il s'agissait du rôle de la culture, de la capacité du soldat et de la possibilité de réseautage. On estimait que RDDC n'était en mesure d'appuyer que le dernier. L'autre équipe a examiné des technologies susceptibles de faciliter la transformation au cours des 30 prochaines années. Elle a déterminé que les systèmes et plates-formes à énergie dirigée, les technologies de cyberguerre, les nouveaux matériaux et les sciences cognitives feraient partie des technologies perturbatrices de l'avenir. Ce sont des technologies nouvelles ou existantes qui sont utilisées d'une manière innovatrice, de sorte qu'elles modifient considérablement les pratiques établies. Les conclusions des équipes ouvrent la voie à d'autres discussions sur la transformation et le futur cadre des sciences et de la technologie.

This page has been deliberately left blank

Page intentionnellement blanche

Executive summary

The Department of National Defence (DND) and the Canadian Forces (CF) are engaged in the analysis of the future defence and security environment and how they must transform to meet its challenges. Defence Research and Development Canada (DRDC) formed two Tiger Teams to develop timely and relevant input into this strategic process, as defence research and development will have great influence on Transformation.

The Transformation Concepts team examined a number of concepts and discovered three pervasive influences: cultural issues, the soldier's capability, and being network enabled. Culture was deemed the most important as it covered all areas from being able to assess intelligence and actions from a cultural perspective to trust issues between humans and machines (e.g. artificial intelligence). The second influence of the soldier's capability dealt with the theme of the Tactically Self-Sufficient Unit (TSSU). Rather than traditional permanent military units, ad-hoc formations would be assembled at short notice. These TSSUs would require specialist soldiers who could quickly adapt to the new structures and mission. The challenge is to field the correct mix of generalists, specialists, or soldiers with both capabilities. The final influence, being network enabled, relates to the concept of Network Centric Warfare. For example, networks will be required as larger numbers of autonomous systems are used and the success of Effects Based Operations requires networked forces in order to maximize the use of all capabilities. Being network enabled is key to knowledge and experience capture and integrated intelligence, surveillance, and reconnaissance. The team found that DRDC's Technology Investment Strategy is well positioned towards this latter influence. Less support is found for soldier's capabilities and even less is provided to cultural issues.

The Technologies for Transformation team examined both battlefield-ready technologies within ten years and disruptive technologies within 30 years. In the first category information and brief analysis were provided on developments in intelligence, surveillance, and reconnaissance; micro-satellites; chemical, biological, radiological detection and protection; autonomous intelligent systems; hyper-spectral sensing; wideband wireless; non-lethal weapons; and ubiquitous modelling and simulation. For potentially disruptive technologies the team examined directed energy systems and platforms (enabled by projected advances in physics, mechanical sciences, material science, chemistry, and electronics); cyber-war technologies (enabled by quantum computing, information proliferation, and the vulnerability of critical systems); new materials (enabled by demand for lighter weight and higher performance which have shifted material programs away from metals and towards polymers, ceramics, and semi-conductor materials); and cognitive sciences (enabled by nanotechnology and brain-imaging technology).

Both teams remarked that the field of study is so broad that a more sustained effort at analysis is required.

Porter, N.R., Kennedy, J.L., Bridgewater, A.W., et al. 2004. Transformation Concepts and Technologies. DRDC TR 2004-003. Defence R&D Canada.

Sommaire administratif

Le ministère de la Défense nationale (MDN) et les Forces canadiennes (FC) ont entrepris l'analyse du futur cadre de défense et de sécurité et de la transformation qu'ils doivent subir pour relever leurs défis. Recherche et développement pour la défense Canada (RDDC) a constitué deux équipes spéciales en vue d'apporter une contribution opportune et pertinente à ce processus stratégique, étant donné que la recherche et le développement dans le domaine de la défense auront une grande influence sur la transformation.

L'équipe des concepts de transformation a examiné un certain nombre de concepts et décelé trois influences communes: les questions de culture, la capacité du soldat et la possibilité de réseautage. La culture était jugée le facteur le plus important, car elle recoupe tous les domaines, qu'il s'agisse de la capacité d'évaluer du renseignement et des actions d'un point de vue culturel ou des questions de confiance entre humains et machines (p. ex., intelligence artificielle). La deuxième influence, soit la capacité du soldat, traitait du thème de l'unité tactiquement autonome (UTA). Plutôt que de compter sur des unités militaires permanentes comme autrefois, des formations spéciales seraient constituées à bref délai. Ces UTA devraient être formées de soldats spécialisés capables de s'adapter rapidement à de nouvelles structures et missions. Le défi consiste à trouver la bonne combinaison de généralistes et de spécialistes ou de soldats ayant ces deux capacités. La dernière influence, soit la possibilité de réseautage, porte sur le concept de la guerre réseaucentrique. Par exemple, des réseaux devront être établis puisque de nombreux systèmes autonomes seront utilisés, et pour assurer le succès des opérations axées sur les effets, il faudra disposer de forces réseautées afin de maximiser l'utilisation de toutes les capacités. La possibilité de réseautage est essentielle à l'acquisition de connaissances et d'expérience ainsi qu'à l'intégration du renseignement, de la surveillance et de la reconnaissance. L'équipe a trouvé que la stratégie d'investissement technologique de RDDC était bien adaptée à cette dernière influence. L'appui est moindre pour les capacités du soldat et encore moins grand pour les questions culturelles.

L'équipe des technologies de transformation a examiné les technologies qui seraient prêtes à être appliquées sur le champ de bataille d'ici 10 ans ainsi que les technologies perturbatrices qui se manifesteront d'ici 30 ans. Dans la première catégorie, on a fourni des renseignements et une brève analyse sur les progrès dans divers domaines: renseignement, surveillance et reconnaissance; microsatellites; détection d'agents chimiques, biologiques et radiologiques et protection contre ceux-ci; systèmes intelligents autonomes; détection hyperspectrale; systèmes sans fil à large bande; armes non létales; modélisation et simulation omniprésentes. En ce qui concerne les technologies potentiellement perturbatrices, l'équipe a examiné les systèmes et plates-formes à énergie dirigée (rendus possibles grâce aux progrès anticipés en physique, sciences mécaniques, science des matériaux, en chimie et en électronique); technologies de cyberguerre (validées par l'informatique quantique, la prolifération de l'information et la vulnérabilité des systèmes critiques); nouveaux matériaux (validés par des exigences de réduction de poids et d'augmentation de la performance qui ont modifié les matériaux faisant l'objet des programmes, ceux-ci étant passés des métaux aux polymères, à la céramique et aux semi-conducteurs); sciences cognitives (validées par la nanotechnologie et la technologie d'imagerie cérébrale).

Les deux équipes ont constaté que le champ d'étude est tellement vaste qu'il requiert un travail d'analyse plus soutenu.

Porter, N.R., Kennedy, J.L., Bridgewater, A.W., et al. 2004. Transformation Concepts and Technologies. DRDC TR 2004-003. Defence R&D Canada.

Table of contents

Abstract i

Résumé i

Executive summary iii

Sommaire iv

Table of contents v

List of figures viii

List of tables viii

Acknowledgements ix

Introduction 1

Transformation Concepts Overview 3

Technologies for Transformation Overview 7

Conclusion 9

Transformation Concepts

Annex A: Some Thoughts on the Problem of Predicting the Future Technological Transformations that will Impact the Canadian Forces 10

Annex B: Human Factors Transformation Concepts 12

Annex C: Network Centric Warfare for Increased Mission Effectiveness 17

Annex D: Effects Based Planning 22

Annex E: Interoperable, Networked Forces in Coalition Warfare 25

Annex F: Network / Information Protection 26

Annex G: Integrated Intelligence, Surveillance, Reconnaissance (ISR): Data Fusion / Mining 30

Annex H: Knowledge / Experience Capture: Lessons Learned and Knowledge Inventory and Control 31

Annex I: Future Autonomous Systems 33

Annex J: Non-Invasive Personnel Identification and Tracking 35

Annex K: Full Spectrum Protection 36

Annex L: Process Improvement 38

Annex M: Footprint Reduction 39

Annex N: Capability-Based Force Development 41

Annex O: Technological Red Team: Threat Exploration 42

Battlefield-Ready Technologies

Annex P: Intelligence, Surveillance and Reconnaissance (ISR) 43

Annex Q: Micro-Satellites 45

Annex R: Wideband Wireless 46

Annex S: Hyper-Spectral Sensing 48

Annex T: Chemical, Biological, Radiological Detection and Protection 49

Annex U: Autonomous Intelligent Systems 54

Annex V: Non-Lethal Weapons 55

Annex W: Ubiquitous Modelling and Simulation 57

Transformational Technologies

Annex X: Directed Energy Systems and Platforms 59

Annex Y: Cyber-War Technologies 63

Annex Z: New Materials 65

Annex AA: Cognitive Sciences 68

Annex BB - Terms of Reference - Defence R&D Canada (DRDC) Tiger Team on Transformation Concepts 71

Annex CC - Terms of Reference - Defence R&D Canada (DRDC) Tiger Team on Technologies for Transformation 72

Appendix A: Transformation Concepts Matrix 73

References 76

List of symbols/abbreviations/acronyms/initialisms 79

List of figures

Figure 1. Network Centric Warfare / Network Centric Operations Conceptual Framework ... 20

Figure 2. Defence related areas that could be influenced in the next 10 to 15 years by material technology research areas.....66

List of tables

Table 1. Characteristics of a Network-Centric Military System 18

Table 2. Technology Investment Strategy 74

Table 3. Transformation Concepts Matrix 75

Acknowledgements

The authors would like to thank Tom Cousins, DRDC Ottawa, and Jocelyn Keillor, DRDC Toronto, for their contributions to the report. As well, thank you to Neil Sponagle, DRDC Atlantic, and Joe Templin, National Research Council Canada (Institute for Aerospace Research), for their participation as Tiger Team members during the workshop (Technologies for Transformation and Transformation Concepts teams respectively). We also thank Orrick White and Abe Jesion from Directorate Science and Technology Policy (DST Pol) for their help in organizing the workshop, providing the secretariat, and helping with the final report.

Introduction

> Future threats will present themselves quickly and asymmetrically. Future conflict cannot be played out as a chess game no matter how sophisticated computing technologies become since the pieces and the board will morph unexpectedly as the game proceeds. The level playing field will no longer exist.
>
> Peter Tikuisis - DRDC Toronto

Transformation is defined as "a departmental process of strategic re-orientation in response to anticipated or tangible change to the security environment, designed to shape a nation's armed forces to ensure their continued effectiveness and relevance." Transformation "does not however seek the complete re-structuring or re-equipping of Canada's military forces, but will instead blend existing and emerging systems and structures to create greatly enhanced capabilities relevant to future missions, roles and tasks." As part of Transformation the Department of National Defence (DND) and the Canadian Forces (CF) are engaged in the production of a series of documents providing strategic direction. These include Strategy 2025 and the Strategic Operating Concept (SOC). Such documents are intended to inform capability based planning and the entire force development process. Once an overall DND/CF strategy is determined, it will have important implications for the future of the CF and ultimately the Technology Investment Strategy (TIS) and the direction of the Research and Development (R&D) program.

In July 2003, the Technology Assessment Working Group (TAWG) sponsored a mini-workshop on the role of Defence Research and Development Canada (DRDC) in Departmental and Force Transformation. The results of this workshop were discussed at a subsequent meeting of the Research and Development Executive Committee (RDEC). In October, the RDEC approved the establishment of two Tiger Teams to contribute timely and relevant input to the development of the DND/CF strategic documents. One team, lead by Jim Kennedy (DRDC Atlantic), would focus on 'Transformation Concepts' while the other, lead by Bert Bridgewater (DRDC Ottawa), would examine 'Technologies for Transformation'. Each team was composed of representatives from each DRDC Centre.

All members of the Tiger Teams attended a two-day workshop at DRDC Corporate in mid-November. The first half-day was a plenary session devoted primarily to establishing a common appreciation of the contextual setting for strategic planning in DND and the CF. Each team then met separately for the remainder of that day and the following morning for a brainstorming session. The results from this meeting were presented to the Director General Research and Development Programs (DGRDP) and to the plenary on the afternoon of the second day. Actions were approved and subsequent analysis was performed on a portal.

Individual members of the team, or other contributors from their home organizations, wrote the separate sub-sections. Unfortunately, there was little opportunity to discuss collectively the statements made. At the end of several weeks' efforts, the findings of the team members were gathered by their team leaders and consolidated into team reports and finally into one Transformation Tiger Team report. This report is composed of the team overviews and their

combined conclusions followed by individual members' essays organized as annexes. These annexes are grouped with the Transformation Concepts first, succeeded by Battlefield-Ready Technologies and then Transformational Technologies. An appendix that illustrates the findings of the Transformation Concepts team is also included.

Transformation Concepts Overview

Information collected

Given the ambitious timelines, to facilitate discussion during the brainstorming session the Tiger Team grouped transformational concepts using broad capability functions. Although this may not have been the most innovative way of looking at things, it proved a convenient way to kick-start the process. The functions used include:

- Knowledge Based Command and Control;
- Integrated Information and Intelligence;
- Generate Forces;
- Sustain Forces;
- Conduct Operations; and
- Force Protection.

Following the brainstorming session, the team members took responsibility for a selection of concepts and prepared essays or commentaries on them. These, in turn, were posted on a portal and each member was afforded the opportunity to expand on these initial thoughts. These descriptions and critiques were then collated and a team overview created.

The two-day workshop that the Tiger Team held produced some 21 concepts and lead to 15 essays. These concepts span a wide range, but cannot be regarded as exhaustive. The use of the portal technology did not lead to any further additions. It is noted that the Analyst on the team was the most active in the portal and produced most of the debate. The variety of styles and presentational format attests to both the diversity of the group and of the concepts.

It had been suggested that overarching concepts should be identified. At first blush Network Centric Warfare might be one and Effects Based Operations another. Such concepts are not easy to define and the essay on Network Centric Warfare points to some of the difficulties in defining that particular concept.

Finally, the reader will no doubt observe that there are recurring themes. The three themes that stand out relate to: cultural issues, the soldier's capability, and being network enabled. The Tiger Team has chosen to label these pervasive influences.

Pervasive influences

Cultural issues

The most pervasive influence identified was understanding cultures. One concept that arose under the integrated information and intelligence capability related to appreciating and adapting to cultural differences. The discussion on this is found in the human factors essay. This underscored the need for scientific research in this field, to understand a diverse spectrum of cultures, both within the Canadian Forces and outside of it. The point was reinforced in the network centric essay. Effects Based Planning involves collaboration and accommodation, not least an understanding of friends', foes' and neutrals' perceptions to correctly evaluate intelligence and anticipate consequences or effects. Knowledge capture and integration of cultural intelligence into plans remains a challenge. The notion of a 'bad guy detector' also has cultural overtones. In sum, it was recognised that cultural, political and military-doctrinal interplay is increasingly significant in coalition operations and may be a serious impediment to the flow of information and shared situational awareness between coalition partners.

The importance of trust is reinforced in the essays on human factors, interoperability and knowledge capture. The first issue relates to trust within our own forces. An assembly of highly trained and diversely skilled individuals with a better than historic appreciation of the operational context may be predisposed to exhibit a more discriminating attitude towards leadership, with the inherent concerns of trust and confidence. This is becoming more pressing given increasing focus on agility and an emphasis on joint and combined operations. Furthermore, units may not be given extended opportunities to train together before being deployed. This leads to the issue of trust within coalitions and between military forces, Other Government Departments (OGD) and Non-Governmental Organizations (NGO). The essay on interoperability concluded that trust might well be a key determinant in the success of a coalition force. When it comes to knowledge capture, the user must be able to anticipate and control the uses to which his or her contributions will be put. Organizational structure must complement the info-structural arrangements and more research is required in this area. A final related area relates to the man-machine interface, the trust between the serviceman or woman and machine. As alluded to previously, the trend is toward system integration, among rather than within, platforms and reliance on external information sources. It is noted that the adoption of artificial intelligence introduces potentially conflicting issues of the delegation and acceptance of responsibility and authority.

In the essay "Some thoughts on the problem of predicting the future technological transformations that will impact the Canadian Forces", it was suggested that the most significant and immediate impact of all future technologies might well be associated with a major shift in the hiring and training practices of the CF. Reference was made to similar cultural impacts on training in the human factors essay. It was also alluded to with reference to integrated Intelligence, Surveillance, and Reconnaissance (ISR),

as it was observed that future soldiers will have to develop the cognitive ability (agility) to handle greater uncertainty.

The Technology Investment Strategy (TIS) is largely silent on the issue of understanding cultures. The TIS does touch on the area of trust in man/machine interactions in the Information and Knowledge Management research area. There, particular emphasis is being given to reducing operator workloads by introducing trusted intelligent assistants. There is also a focus on research in team decision-making, and in trust and confidence in advice in the Command Effectiveness and Behaviour research area. This research area also has application to training where there is uncertainty, which addresses one specific issue noted above. However, understanding and adapting to cultural diversity is not a focussed TIS area.

Soldier capabilities

The concept of Tactically Self-Sufficient Units (TSSUs) was introduced in previous work on capability based planning and was a recurring concept in the essays. Specifically, in the human factors essay, it was noted that large numbers of basic troops would still likely be necessary to support some operations. In other cases, smaller numbers of more specialized members will likely be required. Future TSSUs will likely exist less as a collection of permanent bodies and more as temporary formations assembled from a pool of specialized individuals or small units in response to the task at hand. For such TSSUs to work, the DND/CF must produce and train a serviceman or woman who is a sophisticated specialist in a given field yet also has the flexibility to participate on short notice in ad-hoc teams put together in reaction to a specific situation. Hence they must have the abilities, predisposition and agility to manage the intellectual challenges that will be required of them and to effectively exploit all the assets that will be at their disposal. The TIS does not explicitly address research that meets the challenge of making TSSU functional, although the research areas of Command Effectiveness and Behaviour and Human Factors Engineering seem appropriate areas from which to draw relevant competence.

The essay on autonomous systems gives an indication that some relief to these demands may be in sight. It may be easier to program machines than men to cater for requirements to operate in a variety of complex environments.

Assembling TSSUs has some potential difficulties. The essay on Effects Based Planning notes that, given a situation and desired outcome that calls for specific leadership qualities, skill sets, etc. a soldier would be chosen from a planning tool and assigned the task that they know best to perform in those conditions. The difficulty lies with the question of leadership, it was observed in the human factors essay that the melding of officers and highly educated non-commissioned members might require a re-evaluation of the traditional rank structure within the CF.

Being network enabled

Being network enabled is obviously a requirement of Network Centric Warfare. It is also a key component of knowledge/experience capture and integrated ISR where information is to be captured, fused and used in a timely manner. The human factors

essay also noted the requirement for knowledge that drives being network enabled. The driver is to establish how this knowledge will be gained from the assessment and integration of information collected by the network, followed by a clear commander's intent timely disseminated throughout the network.

The future for autonomous systems will bring a demand for networking to handle the swarms of vehicles that are on the horizon. Effects Based Operations' needs are brought about by the requirement to use coordinated application of all available capabilities, in order to achieve the desired strategic objectives. While interoperability does not demand networkability, the requirement for information interoperability would seem to be better accomplished by a network enabled force. Indeed, a networked force provides an opportunity for familiarity and greater information exchange, possibly leading to a greater level of accessibility of meaning in the information that is passed through the network. The TIS is well positioned to respond to the needs of the CF to be network enabled. There are activities on this topic in nine of the 22 research areas of the TIS. The essay on network/information protection highlights some of the work in the area.

Technologies for Transformation Overview

Two types of technology are useful when discussing Transformation: battlefield-ready technologies and disruptive technologies. Battlefield-ready technologies are those that are Transformation enabling while disruptive technologies are new or existing technologies used in an innovative fashion that significantly alter established practices. Common historical examples of disruptive technologies include the tank and the aircraft carrier. It must be noted that it is not the technology per se, but also the doctrine or emergent concepts linked to the technology that make the system disruptive. In the case of the tank, its disruptive nature only became fully evident once armoured forces were linked with the power of the radio network and the doctrine of *blitzkrieg*. With the increased diffusion of both knowledge and technology it is important that both these technological trends be monitored in order to avoid surprises and to take advantage of opportunities.

Under the heading of technologies approaching battlefield readiness, the team looked at some emerging trends, mostly related to sensors and communications. In Intelligence, Surveillance and Reconnaissance (ISR) the trend will be towards greater security through the use of passive sensing and the watermarking of electromagnetic transmissions. Micro-satellites will provide low cost surveillance capabilities. A wide range of new techniques and technologies in Chemical, Biological, Radiological (CBR) detection and protection will appear. In detection there will be the ability to rapidly sense more varied threats at lower levels as well as possible network and stand-off applications. In protection new, less corrosive, formulations of equipment decontaminant will be developed, as will new antidotes. For Autonomous Intelligent Systems (AIS) possible roles emphasize their surveillance abilities but recognize their limitations due to legal and moral concerns. The pervasive impact of wideband wireless technologies is assessed in light of security concerns. Ultra-wide bandwidth is identified as a means of creating high data, multi-user networks. As well, some growing policy concerns in the area of non-lethal weapons and their use are analysed. The team also revisited the established technology of hyper-spectral sensing which made large gains in the last 20 years and led to improved attribute recognition and situational awareness. Also examined were some of the expectations and real requirements in the domain of ubiquitous modelling and simulation with the admonition to not expect one universal simulation, rather the creation of validated and verified tool kits should be expected. Generally, the treatments consisted of a description or critique of the technology under discussion followed by a short statement on its relevance to defence and security matters over the next ten years. Direct quotations from other sources have been inserted in the text where it was felt they amplified the key points or filled a gap in the overall treatment.

Under the heading of disruptive technologies the team examined four key areas that may have a dramatic impact on future defence and security operations:

- Directed Energy Systems and Platforms – These will evolve out of discoveries in physics, mechanical sciences, material science, chemistry and electronics. New structures, launch capabilities, and kill properties are just some of the developments in this field.

- Cyber-War Technologies – These will evolve from the increasing accessibility of commercially available strong encryption and the concomitant problem for intelligence gathering, cryptographic advances based on quantum computing, and the vulnerabilities of the infrastructure of the global information grid.

- New Materials – This area involves the shift from metals to polymers, ceramics, and semi-conductor materials. These developments should lead to improved performance and reliability at a lower cost. It is also noted that research in civilian sectors such as transport, energy, medicine and health care, etc. will have an important impact.

- Cognitive Sciences – These suggest that brain activity can be influenced in a gross way by electromagnetic stimulation or chemical treatment. Research is ongoing in a number of areas related to both implantable and peripheral devices, the latter is more likely to appear soonest. It remains to be seen if people and society will grant ethical and personal acceptance given these technologies' invasive nature.

In its initial brainstorming session in November 2003, the Tiger Team identified several other technologies that should be assessed for battlefield readiness: fuel cells, psychological operations/perception management, biosensors, and navigation warfare. Time and unavailability of staff precluded their treatment in this report. Several other potentially disruptive technologies might also have been included, for example, nanotechnology or nuclear fusion power, but the four chosen were considered to be quite inclusive in their embrace of the likely future governing features of the Transformation in defence and security affairs, coupled with those technologies discussed under near-term battlefield readiness.

Conclusion

It is difficult to predict the direction of Transformation with any accuracy. Traditionally, the military has been criticized for being conservative, yet when one's decisions can lead to victory or defeat it is perhaps best to tread cautiously. In assessing which concepts and technologies will be critical in the future it should be acknowledged that it is difficult to pick the 'winners'. This report is only a first step at setting out a more comprehensive assessment of the Transformation Concepts and Technologies for Transformation in the Canadian context.

Three pervasive influences that impact on the majority of the concepts were identified. These were; cultural issues, the soldier's capability, and being network enabled. The technologies for Transformation include those that will be ready within 10 years and technologies that may prove disruptive in the future. These disruptive technologies include directed energy systems and platforms, cyber-war technologies, new materials, and cognitive sciences.

Annex A: Some Thoughts on the Problem of Predicting the Future Technological Transformations that will Impact the Canadian Forces

Georges Fournier
DRDC Valcartier

The problem of predicting the future, particularly when technology is a central component, is that we generally proceed by extrapolating directly from the present situation. This might be legitimately called the linear approach. It is generally the best we can aspire to do at any given point in time. However, by far the most interesting thing about the future is that it is essentially non-linear. Technology and science never let us proceed along a single track (however convoluted its path) to a reasonably predictable future. Discoveries, which by their very definition are unpredictable, force us to often jump sideways and proceed forward from thence on an entirely different track. Often, disruptive innovation results from the convergence of several different enabling technologies. It is impossible to track, let alone conceive of, the matrix possibilities.

Notwithstanding Forecast methodologies, we are likely to be continuously blindsided by the more significant parts of our future. This may be particularly true in the military field where a smart enemy will proceed by carefully evaluating what you believe he will do and then, if he can, pursue the unexpected, i.e. do precisely what is unthinkable to you.

The products of technology and, more significantly, the detailed knowledge of the workings of various technologies are increasingly universally and readily accessible. The only prerequisite to exploiting many of these technologies effectively is will and brainpower, and there is no shortage of either commodity everywhere. We are therefore entering the age of the survival of the smartest. Our ability to predict potential threats will diminish and our only reasonable course of action must be to increase our flexibility of response.

After conducting several interviews at DRDC Valcartier on the various discussion items that were assigned to me, this theme of sophistication and flexibility of response surfaced again and again. It was emphasized by several people (working in different sections and fields) that **the most significant, immediate impact of all future technologies will be what might be loosely referred to as a major culture change in the hiring and training practices of the CF.** This is of immediate importance because of the enormous inertia and the long lead times involved. The people we recruit today are ten years from either being directly involved in this process of permanent change or training new people in this way of life themselves. Intellectual agility is the precursor to innovation and organizational agility. A significant contribution by DRDC to the process of transformation could lie in assessing accurately the intellectual burden of the tasks that might be required of DND/CF personnel. What set of abilities, attitudes and training will be required? Tomorrow's scientist and soldier will need to easily absorb and integrate technology in his or her way of life.

The only absolutely reliable prediction we can make for the future is that we will likely have to react promptly. This state of near continuous adaptation, when coupled with ever-

increasing complexity and task training time, creates a quandary. The question we are left with is how to produce and train a soldier who is a sophisticated specialist in a given field and, at the same time, has the flexibility to participate on short notice in ad-hoc teams put together for a specific response. In addition to his or her specialist expertise, he or she must have sufficient knowledge of the other team members' functions to instinctively understand the required interface and procedures to complement them. The development of this independence and uniqueness of the individual soldier while still keeping alive a strong *esprit de corps* will not be a trivial proposition.

We have talked about the LEGO model analogy where each block can have a different function but they all can be assembled in various ways to operate together in different situations. I would hazard to suggest that another equally compelling but truly human analogy is that of the London 'sessions musicians'. These are the highly talented musicians that are brought in to produce recordings on short notice. A famous example from yesteryear is Mantovani's (non existing) Orchestra. These people, even though they rarely see each other and they play very different instruments, manage to integrate themselves on their own quickly (in the matter of minutes not hours) into a cohesive whole and produce a high quality performance. To carry the analogy further, Information Age warfare is more akin to jazz than classical music.

I believe that we now, as a matter of some urgency, have to find a way to elicit the same type of flexible behaviour in our troops vis-à-vis the uncertain technological future. To repeat, a significant contribution of DRDC to the process of Transformation might lie in accurately predicting and updating what set of abilities, attitudes and training will be required of the future soldier. The long lead times make the task difficult but also add an immediate urgency that some other aspects of future technology impact do not have.

Annex B: Human Factors Transformation Concepts

Peter Tikuisis
DRDC Toronto

Objective

The objective of this discussion is to postulate and critique Transformation concepts in a broad operational context. Transformation is the process of strategic re-orientation in anticipation of and/or response to changes in the security of Canada, brought upon by changes in technology and/or threat. DRDC's role is to provide value and leadership to this process at the front end by identifying where our research efforts can yield maximum returns and congruency for an ever-evolving CF. If we are not part of the change, then we will be reacting to change.

Preamble (Setting the Scene)

> The key to future success is to rely less on the attempt to accurately predict the likely requirement and instead to prepare for a range of requirements.
>
> *Duty with Honour - The Profession of Arms in Canada*

Forecasting technological change is less risky than forecasting future threats. Indeed, with the advent and growth of asymmetrical acts of violence, non-state aggressors, and sole perpetrators, mostly unforeseen 20 years ago, it is very difficult to forecast future threat in the 2020-25 horizon with any certainty. Thus, prescribing successful Transformation(s) is especially challenging given this vacuous frame of reference. At best, DND must anticipate broadly, prepare for any eventuality, develop robust contingency plans, and confront asymmetrical threats with asymmetrical action (i.e., avoid being predictable).

Below, suggestions are put forward on Transformation concepts within a human factors context. First, consider the possible direction(s) that DND might follow in the future security environment. On the domestic front, large numbers of basic troops will still likely be necessary to provide security and assistance in emergency situations, whereas smaller numbers of more specialized members will likely be required for localized sovereignty protection (major threats will probably require allied assistance). Similarly, large units of basic troops will likely still be required for continued peacekeeping missions and possible involvement in foreign coalition operations. These activities will undoubtedly be complicated by the operational shift to more complex terrains, and increased contact with non-combatants and refugees. However, it is also quite likely that the proportional representation of troops in these large units will decrease in favour of an expanded and increased use of Tactically Self-Sufficient Units (TSSUs) for rapid deployment and surgical strike assignments. Future TSSUs might exist less as a

collection of permanent bodies and more as temporary formations assembled from a pool of specialized individuals or small groups for the task at hand.

Transformation concepts are discussed along four major themes underlined by the above forecast. Certain of these concepts are presently being researched and will have a transformational impact within 10 years (near-term). The balance, extending beyond 10 years (long term), is obviously more speculative.

Use of Information and Artificial Intelligence for Rapid Self-Synchronization and Decision-Making

Command has always been based on knowledge garnered from information (the two are not synonymous). The striking difference today and more so in the future is the speed and fullness of reports and intelligence that is received by command (at all levels). Perhaps the near-term Transformation will be how real-time inflow of voluminous data will be interpreted and distilled for the commander's use, and how to convey the commander's intent unambiguously at all levels. At issue here is the quality and quantity of data that must be processed, and how it will be presented to gain sufficient, yet accurate, situational awareness in a timely fashion.

While the 'human-in-the-loop' concept should survive in the long-term, human involvement will likely migrate increasingly away from lower levels of decision making. This shift will occur as Artificial Intelligence (AI) matures sufficiently to assist real-time lower level decision making with less risk of error (than if the human was involved) under highly intense engagements. Whether a replacement or aid to command, such a Transformation will require considerable investment in the development of decision making algorithms. Further, the adoption of AI introduces potentially conflicting issues of the delegation and acceptance of responsibility and authority. Who ultimately assumes responsibility for decisions made using AI will be an ever-evolving challenge according to the level of AI use.

Cultural Translation for Effective Defence, Operational Efficiency, and Truly Shared Situational Awareness

With increasing global reach, the CF is and will likely be expected to operate within a very diverse spectrum of cultures in the near and long terms. Understanding cultural differences must be brought to a sufficiently high level so that potential acts of violence and aggression can be pre-empted or diffused with minimal adverse consequences. Cultural knowledge can also be utilized to wage a psychological campaign to shape perceptions and allegiances advantageous to CF members and operations.

Additionally, cultural differences within the CF community will heighten the challenge of assembling TSSUs if a capability-based doctrine is adopted.[1] Research on recruitment, training, and cohesion must be conducted to ensure team capability and compatibility. Further, increased recruitment of highly educated individuals and subsequent training to advance their specialized and sophisticated skills will generate a more discriminating membership with regard to quality of life issues. On the question of leadership, the melding of officers and highly educated non-commissioned members may require a re-evaluation of the traditional rank structure within the CF. Two driving factors in such a re-evaluation appear to be the blurring of the distinction between strategic, operational, and tactical levels, and the requirement for the CF recognition and reward system to address the value of skills versus knowledge.

Cultural differences can also be an impediment to interoperability and network centricity with coalition partners via unintentionally mistaken information exchange. Trust and leadership will be weakened unless those engaged communicate on a common platform of understanding. Future command and control research on this issue should alleviate this risk.

Trust and culture will also play a role in the relationship between the public, the military, and private security companies. The current trend towards the hiring of professional security firms for the protection of individuals and/or infrastructure will undoubtedly impact on the profession of arms. It is conceivable that private forces might evolve to a point where they are employed for military campaigns, whether jointly with regular forces or separately for special operations. The question of allegiance (to state or employer) will undoubtedly raise concerns over the wisdom of their use. If sanctioned, such a transformation would likely change the public's perception of the role of a national defence force and it could cause unease among allied forces.

Simulation, Modelling, Rehearsal, and Training for Force Innovation

DRDC is presently engaged in SMARRT (Simulation and Modelling for Acquisition, Requirements, Rehearsal, and Training) research to markedly economize the development of the skills and capabilities of CF members without compromising their safety or the mission. Near-term developments will lead to distributed simulation, which will enhance interoperability and reduce systems integration problems. Long-term transformational challenges involving

[1] An example of the cultural difficulty of melding different types of units was demonstrated by the recent experience of Israel's Defense Forces (IDF). A mismatch in tempo was revealed when regular and reserve units were mixed during battle. The resultant higher number of casualties suffered by the IDF compared to when only regular forces were deployed in a very similar mission was attributed to the lower levels in speed and aggression characterized by the reserve units due to a lack of specific training. Analysts suggest, however, that reserve units would likely achieve the same level of success as regular units if left unmixed. Warfare in Low Intensive Conflict 2004 Conference, 22-24 March 2004, Tel-Aviv, Israel.

SMARRT might include: i) real-time assessment and forecast of mission status and success; ii) prediction modelling of human behaviour for realistic simulation of combat scenarios; and iii) development of portable micro simulation and modelling systems for individual training and rehearsal on demand to customize the required skill set 'just-in-time'.

The latter Transformation would facilitate the development of versatile TSSUs as a multi-functional (varied skills), multi-dimensional (varied roles – intelligence, warfighter), and multi-adaptable (varied environment) expeditionary force. This enhanced capability concurs with the concept of 'Implicitly Professional Adaptability' to develop a rapidly deployable and surgical strike capability for various mission assignments. Inherent in the generation of such fighting units is the expected level of emotional maturity and intelligence of its members to deal with the element of surprise, whether of a tactical or repugnant nature. Any assembly of highly trained and diversely skilled individuals may also be predisposed to exhibit a more discriminating attitude towards leadership, with the inherent concerns of trust and confidence. Such challenges must be met since appropriate recruitment and training of these individuals might be the best means to advance DND's state of human readiness for an uncertain future security environment.

Enhanced Human Performance for Sustained Operations

Increasingly, military forces are being called upon to operate autonomously for up to 72 hours, and perhaps longer. Research is presently being conducted to enhance the physical and cognitive performance of forces during sustained operations through advancements in hardware, doctrine, and physiological aids. How well an individual adapts to technology and how reliant they become on it might undermine the full benefits of technological change. Attention to the individual's emotional well-being should also be addressed in the near-term to lessen the risk of mission failure due to overwhelming combat stress.

Consideration should also be given to possible disruptive behavioural changes in individuals whose equipment will allow increased physical separation supplanted by close electronic contact. This also raises the issue of whether trust and intent may become compromised when face-to-face contact becomes the exception rather than the rule.

Overlapping Technological Developments

While SMARRT activities will greatly reduce concept development costs, real physical systems will still be required for validity testing to ensure that critical phenomena are not mistakenly omitted in simulation.

Long-term research to advance sustained operations could possibly transcend to an on-site increase in force potency. Such a development might be achievable through a

metamorphosis of resources to target-specific requirements and/or through the use of autonomous combat units (as a force multiplier).

Annex C: Network Centric Warfare for Increased Mission Effectiveness

Jim Kennedy
DRDC Atlantic

With contributions by Mark Hazen, DRDC Atlantic and Doug Hales, DRDC ORD

"Network-centric warfare (NCW) is the central concept driving the current revolution in military affairs." [1, p.1]. Not only must the right information be available to the right person at the right time in the right form, but also it must be put to the right use.

The concept of NCW is distilled in the following definition:

> Network-centric warfare is the conduct of military operations using networked information systems to generate a flexible and agile military force that acts under a common commander's intent, independent of the geographic or organisational disposition of the individual elements, and in which the focus of the warfighter is broadened away from individual, unit or platform concerns to give primacy to the mission and responsibilities of the team, task group or coalition [1, p.34].

In point of fact, there is actually no common definition for Network Centric Warfare because the concept is so high level there is nothing objective to arbitrate between definitions. The United Kingdom (UK) prefers to look at Network Enabled Capability (NEC), suggesting that networking adds value to all functional areas, e.g. Conduct Operations, Logistics, etc. across the spectrum of conflict. Additionally, there is a movement towards the use of Network Centric Operations (NCO) rather than NCW. A Canadian national seminar in November 2003 developed the following definition:

> Net Centric Operations – an approach to the conduct of military operations characterized by common intent, decentralized empowerment and shared information, enabled by appropriate culture, technology and practices.

American, British and Canadian definitions are all subject to vigorous debate. To date, the American focus has been on warfighting at the operational and tactical levels. The British and Canadian definitions suggest that network centricity is more pervasive and explicitly broaden the concept. This is significant because it informs whether exploration of the concept is restricted to theatre level combat operations. Obviously the analytical (R&D) challenge is far greater in the British and Canadian context, e.g. to develop appropriate assessment tools and metrics. Mark Hazen points out that the British use NEC mostly because they are unsure that they can or want to go all the way to the American NCW. By retreating back a level of concept to something they can define they will perhaps achieve something not as revolutionary but it will be graspable and measurable. He also recognizes the idea that NCW is not limited to direct combat. In fact warfare includes all aspects of conflict including preparation for it and cleaning up afterward. In reference to the Canadian definition it can be criticized in that, like many of the other NCW definitions, it selects a number of characteristics that it hopes will result rather than saying what is actually characteristic of the

concept, or giving some idea of what is different from any other warfighting concept. For example, the only defining term is decentralized empowerment, which is really just another way of saying (with some watering down perhaps) self-synchronization - which perhaps is a warfighting concept. Note, that the word network is not used in the definition, then why is it in the term? The first definition provided at least states that networks will be used and that the essential unit will be expanded in a way that is not limited by geography, etc.

Characteristics of many types have been ascribed to network centric systems. These can be viewed as a hierarchy, with physical attributes of equipment at the base and characteristics higher up the hierarchy depending on those at the same level or below (See Table 1. [1, p.5]).

Table 1. Characteristics of a Network-Centric Military System

TOP LEVEL	
Force-Level Characteristics	
Speed of command	Force agility and massing of effects
Self-synchronisation	Shared situational awareness
Effects-based operations	Reachback
Information superiority	Interoperability
SECOND LEVEL	
Characteristics of Decisions	
Speed	Soundness
THIRD LEVEL	
Characteristics of Information	
Relevance, clarity	Secrecy
Accuracy	Degree of interoperability
Comprehensibility	Age, currency
Value	Completeness
Timeliness	Authenticity
Consistency	
FOURTH LEVEL	

General Characteristics of Networks	
Availability	Survivability
Reliability	Coverage, homogeneity
Concurrency	Security
BASE LEVEL	
Physical Properties	
Bandwith, network topology, server speed, etc.	

In terms of transformation, NCW is generally viewed as an overarching concept that encompasses four tenets. These depict the purported benefits of adopting NCW and include:

- A robustly networked force improves information sharing
- Information sharing enhances the quality of information and shared situational awareness
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command
- These, in turn, dramatically increase mission effectiveness [2, p.i].

It remains to prove if each tenet holds true across the spectrum of conflict, and to derive comparative measures for informing balance of investment decisions – the trade-offs between information, personnel and capital programs.

Presented in Figure 1 is another common framework proposed by John Garstka of the US Office of Force Transformation.

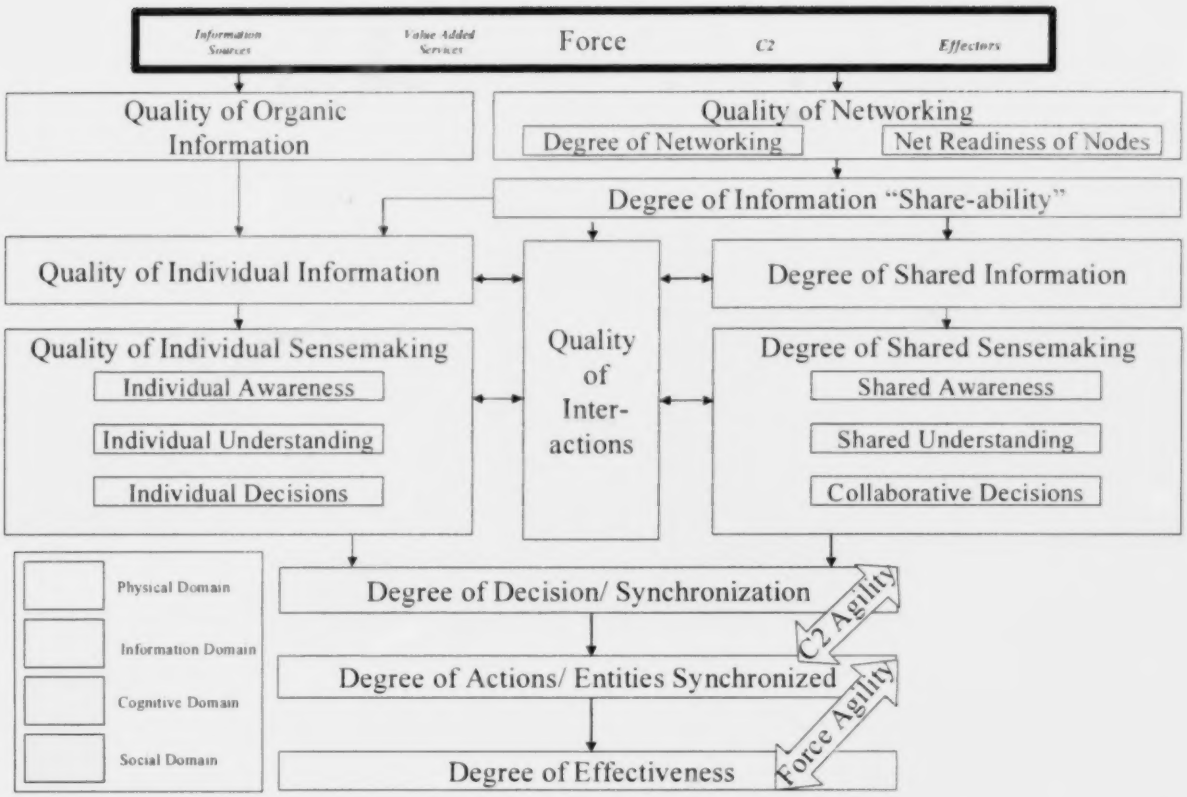

Figure 1. Network Centric Warfare / Network Centric Operations Conceptual Framework

Physical Domain is where strike, protect, and manoeuvre take place across different environments; Information Domain is where information is created, manipulated, and shared; Cognitive Domain is where perceptions, awareness, beliefs, and values reside and where, as a result of sensemaking, decisions are made; Social Domain is where force entities interact [3]

It is particularly noteworthy that this framework has been revised since its inception and now distinguishes cognitive and social domains. The challenge for the R&D community is to apply a systems approach and expand studies on technological support to include the cognitive and social domains. Decision superiority relies on more than information dominance, and perceptions may be as important as 'ground truth' in shaping behaviour.

There are challenges in the path to reaping full benefit of the NCW potential. Excess participation and traffic on a network may reduce its utility. Not all nodes are equal and heterogeneity must be addressed. Improvements in information sharing depend on the quality (raising issues of fitness for purpose and latency) of the information, how we process the information and our requirements for it. Typically decision makers hope more information

will reduce ambiguity. Prior assumptions and expectations can colour analysis. Studies suggest that a few key indicators may be sufficient to generate 'good decisions'. In short, information processing is technology enabled but remains human-centric. Referring to the collective sphere, there is no guarantee that a common situational awareness will be derived from the same information. Even a common situational awareness does not guarantee self-synchronization. Self-synchronization first requires the development of a common culture – tacit values and understanding play a role. How then to proceed?

Annex D: Effects Based Planning

Mazda Salmanian
DRDC Ottawa

With contribution by Doug Hales, DRDC ORD

The term Effects Based Planning is used synonymously with another concept called Calibrated Effects. They are not quite one and the same. Both derive from the development of, and use of, precision weapons in recent conflicts. To execute Calibrated Effects, Force Generation would focus on task tailored forces – military assets would be defined, conditioned, and tested for specific roles. Conversely, the concept of Effects Based Planning envisages the development of versatile Tactically Self-Sufficient Units (TSSUs) as a multi-functional, -dimensional, and -adaptable expeditionary force, i.e. the accent in this case is on task tailored Force Employment. In both instances military assets in question could be tanks, ships, airplanes, communication devices, soldiers, and/or even networks.

These concepts acknowledge the need to improve the capability to respond appropriately and promptly to future threats. Perhaps even more significantly both recognize the need to place the military contribution in context and to coordinate activities with Other Government Departments (OGD) and Non-Governmental Organizations (NGO) to achieve desired effects.

Much like a thermometer that is calibrated and reacts predictably to temperature changes, the military (of year 2025) should have pre-conditioned assets in pre-planned scenarios in order to react quickly, efficiently, and with predictable results.

The development of such 'calibration' or 'effects based planning' presents a formidable challenge. Either requires a mature understanding of causal-effects and a storage facility with sophisticated, cross-referenced identities and capabilities – in effect, an Effect Based Planning Tool. Some of this inventory control may currently be in place, in primitive fashion, for physical and personnel assets that the military operates. In a more tightly coupled world and with increasing reliance on networks and specialists, the demands on the cataloguing and management system have and will continue to increase. Tiered readiness may also have to be factored in. A soldier may be trained in several tactical scenarios; he or she may also have several qualifications applicable at strategic or operational levels. The identity, rank, and capabilities of this soldier need to be recorded and exploited. Given a situation or an event that calls for the leadership qualities, rank, and capabilities of this soldier, and given the desired outcome of the political or military decision maker(s), he/she is assigned the task that he/she knows best to perform in those conditions. Similarly, formations of military groups, to react to an event, will consist of gathering assets via an Effect Based Planning Tool.

Conceptually, an effect based plan will produce quick, efficient, and predictable results. Virtually little is left to guesswork; any activity - be it strategic, operational, or tactical – is surgically implemented as planned. Key assumptions can be tested in scenarios beforehand and plans adjusted accordingly. 'Calibration' requires a context under which testing should occur. Scenarios provide a venue for establishing context and exploring how to achieve predictable and desired results. Thus, aside from training and conditioning, scenarios can play an important part in informing Force Structure. Care must be taken to design complete

scenarios that include options analysis and details of assets use, not just a story line of events. For example, in *Military Wireless Network Information Operation Scenarios* [4], an iterative, cyclical approach to network architecture design within the confines of a scenario is proposed and illustrated in order to highlight the importance of the marriage of technology and the story behind a military scenario. Such a process also compels researchers to note the technical needs of the military in these scenarios. Therefore, scenario creation and design becomes a multi-disciplinary job. A scenario should also be tagged with a (series of) desired outcome(s).

Operational Net Assessment (ONA) can be considered a related and supporting concept. It includes collaborative planning based on potential 'real-world' scenarios and ideally the results feed into national and international crisis contingency plans. The R&D challenges of developing relational databases for tools to facilitate analytical exploration are similar.

Both Calibrated Effects and Effects Based Planning are outcome focussed. This provides the departure point. It is with 'outcome' that decision makers would access the inventory system for assets and scenarios that would result in the desired outcome. Much like a LEGO piece that has a characteristic and can be applied for different purposes, a military asset should be 'tagged' with capabilities and tried in different scenarios for different outcomes. Then the tag must be updated with the successful outcomes and filed back in the Effect Based Planning Tool's inventory system.

A military scenario that is designed for a desired outcome and its corresponding assets must have evaluation criteria [4]. For example, a tactical scenario for a peacekeeping mission will require a secure mobile ad-hoc network. Such a network may be classified and evaluated based on capacity (number of connections or active users), error rate, outage rate (probability of blocking), etc. Such a network should be established based on, and be tested in, a peacekeeping tactical military scenario so that it can be rated and 'tagged' as being an available tool under similar conditions. The military should maintain its readiness with its assets (machinery, networks, etc.), test them in scenarios, and maintain them as deployable-ready. Effects Based Planning with measurable effects reduces the margins of error in military operations and enables more surgical implementation of duties – Effects Based Operation (EBO). Obviously this is easier to do on the tactical level and more subjective on the strategic level.

The Effects Based Operation concept is far broader and more ambitious. An upcoming multinational exercise defines EBO as "operations designed to influence the will of an adversary, one's own forces or neutrals through the coordinated application of all available capabilities, in order to achieve the desired strategic objectives". An effect is "the cumulative consequences across the strategic environment of any one or more actions (or tasks) taken at any level with any Instrument of Government". EBO envisages coordination of diplomatic, information, military and economic levers. Effects themselves can be physical or cognitive. The challenge is to develop causal relationship to achieve precise effects and avoid unintended (and unwanted) secondary and tertiary (i.e. cascading) effects. Precise or calibrated effects are dependent on precise intelligence. This involves an understanding of friends', foes' and neutrals' perceptions. Hence the emphasis on Human Factors and science (vice technology), and interest in complex adaptive systems. Finally it is envisaged that EBO will be scaleable and applicable to coalition operations. Enabling concepts include a Common Information Environment, Integrated ISR, Multilevel Security, a Common

Operating Picture, and Operational Net Assessment (enabled by collaborative planning tools creating virtual teams from dispersed national staffs).

The maturity time line of an Effects Based Planning Tool may be within 25 years; however, the paradigm shift for Effects Based Operations may require more time for adoption in the forces. The implications of this concept are on the military as a whole entity; operations may require army, navy, and air force personnel. Because the military desires to react quickly, efficiently, and with predictable results, the priority of this concept for Strategy 2025 should be high, especially because this concept affects all three documented Courses of Actions (COA) of the SOC. Interestingly, this concept does not change the way a soldier operates in the field. In fact, his or her operations would be surgically designed to be performed easier. Moreover, it will make the CF's coalition activities with allies more effective

Annex E: Interoperable, Networked Forces in Coalition Warfare

Jim Kennedy
DRDC Atlantic

"NATO defines interoperability as 'The ability of…forces…to train, exercise and operate effectively together in the execution of assigned missions and tasks'" [1, p. 13].

"Interoperability is usually viewed as primarily an issue of equipment and the interchangeability of consumables and spare parts, and only secondarily as the commonality of information-exchange protocols." [1, p.13]. Equipment interoperability can be engineered but information interoperability is more complex. The degree to which platforms are able to exchange information is a technological issue. "Security issues, which may be very significant in coalition operations, also affect information flow. Beyond this are cultural, linguistic, doctrinal and terminological issues that determine the degree to which information that is exchanged is comprehended and effectively used." [1, p.14].

Ease of information flow is a prerequisite for networking. "It is conceivable that an increase in the level of networking may help to raise the level of accessibility of meaning in the information passed, simply by providing the opportunity for greater familiarity and exchange of information between units. Insofar as this happens, information-usage interoperability can be viewed as an emergent property of network centricity." [1, p.14].

"Interoperability can be an issue even in single-nation joint-force operations, but it is a crucial aspect of the coalition operations that are commonplace in modern warfare. Usually cultural, political and military-doctrinal aspects are rather more significant in coalition than single-nation operations and security concerns may be a serious impediment to the flow of information between coalition partners." [1, p.14].

"One of the most significant constraints on the success of coalition forces concerns the principle of unity of command; political considerations often prevent the appointment of a single commander with unfettered authority over the whole force … Even if a unified command is established, the degree of subordination of units in a coalition force can be lower than that in a single-nation force; units of nationality different from that of the commanding officer might of their own accord choose to leave the battlespace … Also, national leaders may choose to remove some or all of their units from the coalition at any stage." [1, p.15].

"There can … be an issue with lack of inter-service trust in a joint force, but trust may well be a dominant issue in a coalition force. With current security practices, there are almost certainly categories of information that one nation would not be prepared to share with one or more coalition partner. This compromises shared situational awareness and makes it difficult to establish a Nelsonian 'band of brothers' across the whole coalition." [1, p.15].

Annex F: Network / Information Protection

Mazda Salmanian
DRDC Ottawa

The Canadian Forces command staff require accurate awareness of the Information Technology infrastructure (IT) that are used for operations. They require clear and timely indicators of network attacks, compromised services, and degraded conditions. The Joint Network Defence and Management System (JNDMS) provides such situational awareness [5].

Network defence situational awareness is currently achieved through the combined activities of several organizations. This divided responsibility leads to slower response, and incomplete awareness. Instead of the many localized activities that provide this service now, the Department of National Defence needs a national approach for network defence with the following highlights:

- Data Integration – Increased availability and correlation of network configuration, military operation, and incident data using a unified database;
- Operation Centric Defence – A clear understanding of the overall effect of the IT infrastructure on operations;
- Visualization – A clear picture of the IT infrastructure, and its threats and vulnerabilities;
- Severity Assessment – Introduction of a means to calculate network incident severity taking operational requirements into account;
- Interoperability – Establishing interfaces with coalition partners to exchange infrastructure status and incident data; and
- Preparedness – Improving response time by reducing the diversity of tools employed for data collection and by automating some analysis functions.

Data Integration and Severity Assessment are the most important initiatives. Interoperability will be developed in cooperation with coalition partners. The Preparedness changes will be introduced through the gradual elimination of non-helpful tool diversity.

The JNDMS will be strictly a monitoring system that provides situational awareness. It will not include processes to repair and maintain the network. Such processes are being introduced by other initiatives, and may be integrated with JNDMS in the future to provide a full cycle of detection and response.

The JNDMS Technology Demonstration Program (TDP) project will demonstrate the feasibility of:

- Providing network defence situational awareness to commanders;

- Making this awareness operation centric; and
- Extending it to include coalition partners.

The system will combine and correlate security incident data generated by security monitoring tools, operations data delivered by DND planning activities and Command and Control Information Systems (C2IS), and the IT infrastructure status data, to create the situational awareness needed for network defence.

DND has specific constraints that apply to the transfer of data across security domain boundaries. JNDMS will be designed to accommodate this constraint. These transfers will use one-way only trusted data-diodes. JNDMS will push data periodically from lower level to higher-level security domains. The complete view of all DND networks will only exist at the highest security level.

Network awareness can be improved by correlating incident data with geographical references. A key characteristic of the JNDMS user interface will be the overlay of IT infrastructure data on map backgrounds to provide a visual correlation of places and events.

The JNDMS implementation will be modular, consisting of:

- A distributed database that holds the current status of the IT infrastructure to the extent that it is known at a given location;
- Security event data collection and conversion to the JNDMS schema;
- Operations data collection and conversion to the JNDMS schema;
- Facilities for sharing information with coalition partners;
- Data display functions for user interfaces based on geographical references;
- Incident recognition that accommodates planned outages;
- Severity calculations based on operational priorities; and
- IT infrastructure data collection and conversion to the JNDMS schema.

The JNDMS will run as a collection of nodes with replicated data at each node. If a network is partitioned as a defensive action, the JNDMS services will continue in each of the subnetworks, using the best data available. Later on, when the partitioning is removed, the various JNDMS nodes will resynchronize to restore a complete picture of the network. JNDMS users will have the ability to narrow their view to a specific area of interest, without restricting their ability to see all the available data.

JNDMS is a trust enabler for Network Centric Warfare initiatives within DND. It will underlie improvements in the Canadian Forces Network Operations Centre (CFNOC) such as:

- Shortened response time;
- Better decision quality;
- More flexible response patterns; and
- Increased positive control.

JNDMS will create a common approach for IT infrastructure organizations. The CFNOC will evolve from its data aggregation role to a true network defence authority. JNDMS will provide a system that enables decision makers to more effectively assess the impact on operations of incidents within the IT infrastructure. The benefits include:

- The IT infrastructure status data will be widely distributed and replicated, allowing many different centres to use it as they respond to events. This makes the total response diverse and robust since analysis can continue following the defensive isolation of a domain. The result will be faster defensive actions and improved decision accuracy based on more up to date information.
- The dependence of operations on infrastructure services will be explicitly recorded in the JNDMS database. This will allow the importance of a service for an operation to be queried. This information will lead to more complete network defence situational awareness for operational command staff if there is a loss of some networked components. It will also lead to less disruptive scheduling of maintenance activities.
- For JNDMS the physical location of network elements will be available, and the network diagram will be overlaid on a map background using Geographic Information System (GIS) technology. This will provide a much better means to assess the infrastructure status since queries by location will be supported and the consequences of a problem at a specific location will be better understood for an operation, in particular for deployed units.
- JNDMS will improve incident response times, while making these responses less disruptive. And through a process of integration with JNDMS there will be a shift to the use of the most effective tools. JNDMS will also benefit from automated and dynamic data generation, leading to more complete data being available. Training will be simplified, and the ability of different centres to collaborate will be improved as a result of this data integration.
- JNDMS will address some of the issues involved in coalition participation such as a standard information technology architecture data format.
- The JNDMS database will contain historical data about the network status and defensive posture. It will also keep track of planned infrastructure changes. This capability will support problem management and trend analysis, and improve the ability to plan maintenance so that it minimizes operational impacts.

The Joint Network Defence and Management System (JNDMS) is a TDP implementation of a service that will provide this situational awareness. The JNDMS TDP is an initiative of the Network Information Operations (NIO) Section at Defence R&D Canada - Ottawa. It is a 5-year project ranging from the definition phase starting in FY03/04 to the transition phase ending in FY07/08.

Annex G: Integrated Intelligence, Surveillance, Reconnaissance (ISR): Data Fusion / Mining

Georges Fournier
DRDC Valcartier

The field of data fusion mining has so far exploited with success what might be referred to as well structured situations. For example, taking the inputs from many different sensors and producing more reliable track and identification information. The current trend for research is in the field of integrating non-structured information from all potential sources (images, videos, human intelligence, lessons learned, news, etc). In order to perform this task software will have to be designed that understands the situation for which the fusion is requested and also the context of the user. The results must be tailored to the individual decision-making and cognitive processes of the user. This implies that methods will be developed of dynamically understanding the background and previous knowledge base of the user along with the current context of his or her queries.

The software will also have to be able to gather and quickly sort information relevant to the situation under analysis from the vast pool of external data (broadcasts, internet, etc). This requirement to interface with the enormous pool of information outside DND also implies that secure methods and software will have to be developed to interface effectively with the outside world. These security and openness issues imply that the CF will be forced to rely on special (non-commercial) operating systems or versions thereof that create a secure and reliable known cradle for fusion and mining application.

Ultimately, the complexity of the situations analyzed and the enormous multitude of options that will need to be taken into account and whose solutions need to be optimized make this type of work a candidate that could benefit from the development of quantum computing. Quantum computing, on top of its capability of instant decryption of public key systems, could also be particularly well suited to the solution of optimization and probabilistic problems and might on the long term be used to great profit in this type of application.

One development that will have to occur is more cultural than technological in nature. Future soldiers will have to learn to accept and cope with uncertainty much more than they do today. Current systems do not assign and distribute probabilities very well. They round off to some extent and, for example, often only report the target with the highest probability. This creates an impression of certainty in the user. Even though some options have low probabilities they should still be considered in cases were the consequences would be drastic if they were in fact the reality (e.g. an incoming target has a 10% chance of being a civilian airliner). Significant judgmental errors can occur if the user does not properly digest accurate information and the subtleties of probabilities. This change implies the same comments made on other issues about the problem of hiring, training and retaining appropriate personnel obviously apply in this case.

Annex H: Knowledge / Experience Capture: Lessons Learned and Knowledge Inventory and Control

Georges Fournier
DRDC Valcartier

In general terms, the field of knowledge/experience capture tries to establish a complete cartography of both the acquired and required information of an organization and to ensure easy, fast and effective access and exchange of it. Given the ever-increasing amount of data and the ever-changing nature of the methods of its use, this is far from a trivial endeavour. A flavour for the full complexity of the task can be ascertained by considering the recent developments in the field of Internet search engines. Even though there was a tremendous amount of investment by many companies over the last few years, very few truly effective search techniques were found. As evidence of the difficulty of finding efficient methods one can note that presently one search engine has succeeded in dominating by a wide margin all the others (Google) and it of course keeps its techniques and algorithms secret. Ongoing intense R&D in this field can thus be expected over the course of the next two decades. It is an area where DRDC will be able to find significant inputs from technology developed by the private sector.

For example, the current success of the Google search engine is substantially due to the methods they have found to rate the reliability and usefulness (i.e. the information value to the user) of the various references. Following this trend we will be moving from data retrieval to information retrieval. For a given user, information is the data on a subject that he or she does not already know. In general the field will be moving from serving up data to serving up information. This implies that methods will be developed of dynamically understanding the background and previous knowledge base of the user along with the current context of his or her queries.

There will be some significant special issues in the use of this knowledge technology by the CF. The first of these is the trade-off between openness and security. The security issue is taken here in a broader context than usual. It is first taken to mean both the classic security of having the freedom of consulting or inputting any data the user wishes by any means without compromising the integrity of the user's system or network. It should also be taken in the sense that the user can in all circumstances know, trust and control the uses to which his or her contributions will be put to. The second will be immediate integration of whatever new working customs arise among the younger generation (messenger services and chats presently come to mind) in order to keep and generate the attention of new technology savvy personnel. Personnel who have been able to quickly integrate and use new technologies are precisely the type of flexible and knowledgeable individual that will be needed in future CF operations.

The security and openness issues imply that the CF will be forced to rely on special operating systems or versions thereof that create a secure and reliable known cradle for whatever new functionalities or working customs arise. The CF will therefore be forced to rely less and less on commercial systems. This will imply a substantial increase in software investment. The same problem will face our allies and here again the security issue will reappear when

considering secure interoperability. The combination of security and interoperability will be an even stronger driver and constraint that will lead significant Canadian software investment if we wish to ensure completely secure Canadian operations in an interoperable context. Otherwise, in the near future we need to decide whether we are prepared to take the risk of either buying from or co-developing this specialized software with our allies. Presently, this field drives no major hardware investment.

The same comments made on other issues about the problem of hiring, training and retaining appropriate personnel obviously apply in this case.

Annex I: Future Autonomous Systems

Doug Hanna
DRDC Suffield

Today's joint and combined (US, western, NATO, UN) military capabilities target enemy centres of gravity in conventional operations (outdoor, open engagements) to great effect. The trends of increasing urbanization, ubiquitous communications, and the proliferation of Weapons of Mass Destruction (WMD) indicate that, increasingly, future centres of gravity will be individual combatants or terrorists who will utilize the asymmetric advantages provided by locating themselves in urban areas. Other centres of gravity are increasingly using cover and concealment provided by complex and remote mountainous terrain. Future autonomous systems will be a countermeasure to these threats.

Future autonomous systems will be used to dominate the urban battlespace by utilizing superior future sensing systems, through sheer numbers of systems (system of systems) employed, by utilizing a multitude of building access points when prosecuting operations building by building, and through novel manoeuvre once inside buildings. These same characteristics will permit autonomous systems to detect and identify small pockets of combatants located in difficult terrain. In a protection role, future multi-agent autonomous systems will effectively enlarge the protection sphere around high value maritime assets or homeland installations.

Some of the characteristics of future autonomous systems are:

- Large numbers – 10's, 100's, 1000's, 1,000,000's. While there is value in having individual autonomous systems replace individual soldiers in performing today's dirty, dangerous, or dull tasks, their full value will be exploited when future heterogeneous multi-entity autonomous systems are engaged in new ways. Not merely swarms, but also individually smart in volumes. Swarms are intended to take advantage of the serendipitous benefit of emergent behaviours arising out of dumb autonomous entities. While this may be used to effect in the right circumstances, future autonomous systems will have numerous smart entities possessing superior sensing: multi-spectral, fused, beyond human.

- They will be low cost and disposable in high intensity operations.

- All knowing – Or, at least, 'mostly' knowing via superior sensing for manoeuvre, for multi-agent detection (CBRNE - Chemical, Biological, Radiological, Nuclear, Explosive), for 'bad guy' detection, for the application of lethal force, large database connectivity, etc. They share knowledge – what one entity knows they all know.

- Capable of operations in complex environments – Airborne, or ground assets with excellent manoeuvre capabilities in difficult mountainous terrain or capable of movement in numbers in building Heating, Ventilating, Air-Conditioning (HVAC) ductwork, sewage tunnels, through windows (i.e. every window?) as well as roof access points, etc.

- Learning, adapting machines – What one entity learns, they all learn/know.

Annex J: Non-Invasive Personnel Identification and Tracking

Doug Hanna
DRDC Suffield

In the future security environment, increasing urbanization, ubiquitous communications, and the proliferation of WMD indicate that future centres of gravity will be individual combatants or terrorists located in urban areas where they will be co-located with numerous non-combatants. Since geographical separation is no longer a discerning factor in locating and dealing with combatants, a system for non-invasive personnel identification and tracking, or a 'bad guy detector', would be a useful tool for pointing out which individuals would do us harm.

Characteristics

- Non-invasive, stand-off, possibly remote;
- Stationary for homeland defence applications; and
- Mobile for warfighting, peacemaking, peacekeeping, particularly in urban operations.

Ascending Scale of Capability

- Uniform detector (i.e. type of military uniform – useful, perhaps, in urban operations where non-combatants are also present, but only if they have not doffed them for civilian attire);
- Weapons detector/locator (type? loaded? recently used? where located?);
- Facial recognition, tracking, databasing (have seen him before, know who he is, know where he was, etc.)[2];
- Detects past acts, non-contact and non-invasive? (Detects past acts of interest – i.e. detector knows, from individual's own memory, what combatant/terrorist things he did in the past);
- Detects intentions (is the intent to do harm?); and
- Fuses past acts with associated intentions.

[2] Canadian real time facial recognition research is currently ongoing at such companies as INO. Online at http://www.ino.ca/en/PDF/vga12000.pdf .

Annex K: Full Spectrum Protection

Georges Fournier
DRDC Valcartier

Limited full spectrum protection sensors will probably be achieved within the 2025 time frame. There is a plethora of technologies being developed towards this aim. However, the amount of camouflage, armour or protection will always be limited and weapons will obviously evolve to take into account the protection measures. What we will achieve is more effective cover. One of the concerns relating to Network Centric Warfare is that protection is being sacrificed for situational awareness, increasing the reliance on pre-emption. Arguably, Canadian troops should be prepared to absorb the first shot in many cases. However, we cannot expect anything close to near perfect protection. The only way to be truly safe will be not to be in harm's way (the don't be there doctrine). This approach implies extensive use of remote detection and robotics (both air and ground based).

It should be noted that the approach of not being there will not always be possible to apply, particularly in peace support missions since presence is often a requirement to establish confidence on the part of the local population. As well, effective protection must be offered to that same local population and NGOs in order to secure their aid and participation, which in itself augurs for a broader view of protection. In that case the problem of full spectrum protection remains a vital issue.

The development of armour and camouflage will depend heavily on new materials research. New fibres (e.g. spider silk produced by DNA modified organisms[3] or nanotube fibre systems) as well as polymeric and ceramic multi-impact resistant materials will be developed. This fine tailoring of materials will be driven by the enormous recent increases in both the understanding and modelling of the solid-state and in the development of DNA tailored organisms.

For camouflage and armour, active systems will be developed. The soldier's suit and the vehicle covering will exhibit chameleon-like properties across the Electro-Optical (EO) spectrum. This will require redirecting energy in a patterned way across the vehicle or the suit.

For vehicles very fast, hard kill active armour systems and electronic armour (capacitive melting shields) will be developed and will be coupled to extensive incoming target detection systems with fast reaction times.

Regarding Nuclear, Biological, Chemical (NBC) threats the first level of protection will again be long-range remote agent detection and identification as well as accurate propagation prediction models (i.e. the don't be there doctrine). Reactive neutralizing materials and self-decontaminating surfaces on military platforms will offer the second level of protection. If all

[3] For an example, see the work on ballistic applications of spider-silk fibre conducted by NEXIA Biotechnologies and supported by DRDC. Online at http://nexiabiotech.com/en/00_home/index.php .

else fails, comprehensive personal archival devices will help medical personnel to accurately identify exposure and treatment.

Finally, some system may have to be developed in the future which will offer theatre protection – a so-called Weapon of Mass Protection. An embryonic example would be the American anti-sniper system. A laser microphone can locate a sniper's location by analysing the timing differences of sound. Just one system should be able to monitor most of a large city [6].

All of the above developments imply that both the individual soldier and the vehicles will have access to low weight, high capacity energy sources. Surprisingly, the pace of development in this area is, and probably will be for the foreseeable future, the true technological bottleneck to achieving at a reasonable cost full spectrum protection over extended periods of time. To keep the weight to manageable proportions, effective energy generation systems will need to take full advantage of locally available materials (for example direct electrical generation from bacteria). As it could be the restricting factor for the effective deployment of many technologies currently being investigated or developed by the agency, this energy issue should be tackled by DRDC.

Because of the impossibility of assuring perfect protection, the counterpart of the protection studies must be an effective and accurate threat prioritization system that allows the military to focus on countering the highest risk factors. A concept might revolve around tools (e.g. technology war gaming) and processes to expand, exploit and apply a technology watch.

The aspect that must be looked at in the near future is the set of abilities that will be required of the soldier to effectively use all the assets that will be at his or her disposal (level of education at hiring, training, attitude to continuous learning, etc). DRDC could significantly help in predicting more accurately what the future situation will be and what skills and attitudes will be required to integrate these continual changes. Because of the long lead times this probably needs to be addressed sooner than other issues.

Annex L: Process Improvement

Doug Hales
DRDC ORD

Supply Chain Management (SCM) started as a practice in 1990 and DND was quick to follow industry lead in exploring SCM. In the business world, vendors began to leverage technologies such as advanced optimization algorithms to provide customers with tools that went beyond transaction support and planning solutions that largely fell into two areas: *supply chain planning* and *supply chain execution* (which included warehouse management systems, transportation management systems and order management systems). Many of these solutions have matured to the point of commoditization. However, new applications and enhancements to current solutions are maturing to provide more cost savings and to enable more agile supply chain structures. Some examples of these solutions are:

- Anticipatory Demand/Anticipatory Diagnostics – Forecasting is a technique that is a 'best practice' in the business community that enables this concept. It is similar to the concept of commodity 'push' rather than 'pull' and has the potential to reduce the footprint of the sustain trail. However, a balance must be struck between hedging and reliability of speed and access. The concept requires extensive reliance on:
    - Forecasting algorithms;
    - IT tools and support;
    - A reliable communications system; and
    - A reliable transportation system.
- Real Time Planning – This idea uses applications that balance the supply and demand of goods and services as events occur. These solutions employ repair algorithms, simulations and real-time integration architectures to solve problems as soon as they recognize that something has changed.
- Adaptive Supply Chain Execution – Sophisticated supply chain execution tools that incorporate real-time decision support into supply chain execution processes, enabling re-optimization of the supply chain in near real time, and enabling enterprises to respond to demand volatility without increasing inventory.
- Dynamic Logistics Network Configuration – This is a system or group of systems that enables evaluation of specific orders, and coordinates the configuration of assets and business processes that are on demand within the enterprise and the extended supply chain. The intent is to deliver a specific bundle of products and services.

Annex M: Footprint Reduction

Doug Hales
DRDC ORD

Exploring Footprint Reduction is based on the premise that the quantity of goods required to support any operation drives the requirement for personnel, based on accountability and handling requirements and that the weight and volume of those goods drives the requirement for warehousing space and materials handling equipment. Each of the foregoing contributes to a whiplash effect along the entire supply chain that drives the cost of providing the necessary supply management and transportation services higher.

The meaning, therefore of 'Footprint Reduction' is:

- Reduce the demand for items, thereby reducing the mass and perhaps the length of the supply chain; or
- Enhance the 'potency' of the commodities being considered such that more value is provided per volumetric or weight measure. It is anticipated that this approach will also lead to a reduction in the mass and length of the supply chain.

We will explore concepts and technologies that might lead to a reduction in the demand for these historically resource intensive commodities, specifically, those items that the military refers to as combat supplies:

- Ammunition;
- Rations;
- Water; and
- Petrol Oil Lubricants (POL).

Sample technologies for exploration include, but may not necessarily be limited, to the following:

- Coatings (drag, camouflage, etc.);
- POL Reduction Technologies;
- Hydrogen Extraction and Storage Technologies;
- Ammunition Reduction Technologies (above and below water);
- Ship Automation Technologies;
- Wells, Water purification, Water production;

- Beamed Energy Transfer;
- Internal Combustion Engine Replacement (maintain existing fuel supply chain, but use less fuel);
- Camouflage, Armour, Stealth;
- Holograms; and
- Self-diagnostic, Self-maintaining Equipment.

Additionally, given that sustain in DND terms incorporates Medical and Dental, we will also explore the state of technologies that may include:

- Performance Enhancements (biotech: bio and mechanical);
- Narcotics/Pharmaceuticals;
- Blood Products; and
- Medical Equipment.

Annex N: Capability-Based Force Development

Doug Hales
DRDC ORD

A capability-based approach to force development has been proposed. It is envisaged as:

1. A response to geopolitical and environmental imperatives, business practices, and societal expectations;

2. An intellectual framework for integrating multidisciplinary perspectives, fostering innovation and promoting program coherence; and

3. A communication tool as a means of explicitly linking decisions to policy and relaying that linkage to external and internal audiences.

Capability-based planning inherently recognizes the interdependence of systems (PRICIE components[4]). To this point capability-based planning is more a visionary touchstone than institutional practice. More effort is required to transcend planning, integrate lessons learned from the field and relate generic capability requirements to platforms and units. The objective is to realize capability engineering and capability management. This will require tool and process refinement including development of a methodology for conducting outcome-oriented capability audits and performance monitoring, and a means to seamlessly combine subjective judgement and objective data. This will include maturation and acceptance of soft operational analysis techniques and development of software for translating capability requirements into system and platform/unit details specifying personnel, equipment, infrastructure, and national policy implications. The combination must enable exploration of alternatives/options analysis and related PRICIE implications.

[4] PRICIE – Personnel (including professional development and leadership); Research & Development/Operational Research; Infrastructure & Organization; Concepts, Doctrine and Collective Training; Information Technology Infrastructure; and Equipment, Supplies and Services.

Annex O: Technological Red Team: Threat Exploration

Georges Fournier
DRDC Valcartier

We are condemned to be permanently blindsided by the more significant parts of our future. This is particularly true in the military field where a smart enemy will proceed by carefully evaluating what you believe he will do and then, if he can, do precisely what is unthinkable to you. The unpredictable nature and inherent non-linearity of the future can play havoc on planning procedures unless mental resources are assigned to grapple with the possible outcomes. When it was developing the control program for the space shuttle, IBM gave to a group of scientists, engineers and programmers, comprising 10% of the total personnel involved in the program, the task of making the system fail. The bigger the failure the bigger the kudos and bonuses they received.

We now need to try to do the same thing and attempt in a **determined and sustained effort** to anticipate new devious and dangerous uses of current and future technologies to attack our country and/or our troops. This could take the form of a technological 'red team' whose mandate would be to elaborate methods of inflicting maximum physical and psychological damage to Canada. Some known operational research techniques can be applied immediately to help alleviate the problem but a more extensive effort will be required on the long term.

To be even mildly credible an effort of this type needs to be sustained on perhaps a permanent basis. One cannot come up with truly unexpected credible ways and means of carrying out havoc in a part of this country by an occasional war game. To be efficient, a core competency must be established and maintained along with rigorous records of ideas explored and lessons learned. Substantial input from outside the department and DRDC should be required. This is a case were we really need to think outside the box! People who use their imaginations professionally to produce books, television shows, movies and play scenarios and writers of science fiction could be a good source of potential input to such an activity. A scenario similar to 9/11 can be found in Tom Clancy's book *Debt of Honor* written several years before. I am not sure the terrorists did not actually find their inspiration there.

DRDC's role could be as a moderator in proposing an accurate inventory of present and future technologies and in evaluating the technological and practical feasibility of suggestions from the outside sources mentioned above.

The ultimate aim of this work would be to find ways of countering such schemes either by developing appropriate technological responses or means of early detection of activities and behaviours that would indicate the intention of, or preparation for, carrying out such threats.

Battlefield-Ready Technologies

Annex P: Intelligence, Surveillance and Reconnaissance (ISR)

Pierre Lavoie
DRDC Ottawa

Trend from Active toward Passive Sensing for ISR

Description: As the shift continues towards wireless communications (for convenience and cost-effectiveness) and network enabled systems (for performance), the occupancy of the electromagnetic (EM) spectrum will increase. The current EM spectrum is very poorly used. Monitoring of large systems indicates that the EM spectrum is mostly empty. Policy and regulations for EM spectrum usage will eventually shift from static frequency allocation to dynamic on-demand allocation. In ten years there will be orders of magnitude more communications and active sensor transmissions to intercept.

As a result, it will be possible to carry out many of the intelligence, surveillance and reconnaissance functions passively. Targets of interest include indoor and outdoor communications systems, weapons systems, air defence systems, navigation devices, transponders, etc. Passive ISR will be able to rapidly locate transmitters both indoor and outdoor with targeting accuracy, and track them using electronic fingerprints. Air defence systems that operate entirely passively are already available (e.g.VERA-E).

Defence Relevance: Allies' equipment will transmit only when truly necessary, remaining quiet most of time. The CF and allies will have sensor suites that provide situation awareness by relying on environment transmissions (not their own) . Rapid (seconds) targeting accuracy location (metres) of transmitters will become a reality. Opponents will have this technology too. Hence, the CF will be subject to passive detection and targeting.

Watermarking of Electromagnetic Transmissions

Description: A watermark is a feature on an object that makes it difficult to copy. This feature can be hidden so as to be difficult to detect. A watermark allows the originator of an object to recognize it from copies. Digital image and signal processing will allow watermarking signals transmitted in the EM spectrum.

Defence Relevance: Allies will likely watermark their EM signals and use this technology to recognize each other (combat identification), detect and reject decoys and counter jamming.[5]

[5] Watermarking addresses information terrorism and could potentially avoid scenarios such as terrorists intruding on radio frequencies and causing air collisions. For such a scenario see Devost, M.G., Houghton, B.K., Pollard, N.A. (1996). Information Terrorism: Can You Trust Your Toaster? (Online) Institute for National Strategic Studies, National Defense University http://www.ndu.edu/inss/siws/ch3.html (4 Feb. 2004).

Annex Q: Micro-Satellites

Pierre Lavoie
DRDC Ottawa
With contributions by Bert Bridgewater, DRDC Ottawa

Definition: Micro-satellites have a mass of between 10 and 100 kg,[9] they can be active on orbit for less than $20 million, and they have typical design lifetimes of two years. For the next five years typical payloads will be small passive optical systems, small active optical systems, passive Radio Frequency (RF) systems (e.g. for signals intelligence - SIGINT) and science packages. In the longer term (5 to 10+ years), advances in autonomous space control will allow small clusters of micro-satellites to be integrated as virtual sensors for improved performance and may allow some radar applications. Optimistic projections from the Canadian Space Agency (CSA) suggest that commercially useful Synthetic Aperture Radar (SAR) systems in this domain will be feasible in the 2010 time frame. Forward-looking investigations at DRDC suggest that modest full-function Ground Moving Target Indicator (GMTI) sensors in the small satellite class may be feasible by 2015. Limited-capability, small (approximately 300 kg to 700 kg), high resolution, radar satellites are currently feasible (e.g. the German SAR Lupe or the Israeli TECSAR). The British Joint Doctrine and Concepts Centre argues that, "The space environment **will** be more widely utilised militarily and commercially. This **may** reduce the near-absolute advantage of the US and its allies in this environment before 2015, in terms of communications, positioning and imaging. Space exploitation is **likely** to be more crowded and contested militarily, using both space and terrestrial systems by 2030." [7]

Defence Relevance: Owing to their low cost, micro-satellites bring covert intelligence and surveillance within reach of small countries, private groups and transnational networks. The CF will be working with allies and against adversaries that will have this technology. Missions of interest to the CF include surveillance of space (satellite monitoring and possible ballistic missile applications), low-resolution earth environment monitoring (hyper-spectral applications) and tracking and identification of RF emitters on the earth's surface.

[9] Satellite classification is as follows: pico-satellites have a mass of less than 1 kg, nano-satellites are in the 1-10 kg range, micro-satellites are in the 10-100 kg range, small satellites are in the 100-1000 kg range, and large satellites have a mass in excess of 1000 kg.

Annex R: Wideband Wireless

Daniel Charlebois
DRDC ORD

Description: Wireless communications have become one of the main communication tools used by all military forces. The technologies currently deployed include short-range radio to satellite communications using low-earth orbit platforms to geo-stationary vehicles. Currently, short-range devices typically allow voice communication only. Wireless data networks are still the subjects of R&D. Although the deployment of wireless data networks is currently possible, the high level of security required for military applications have not all been resolved. Other wireless data networks currently rely on either low earth orbit platforms (e.g. Iridium which requires a network of vehicles to ensure uninterrupted service orbiting at 500 to 3 000 km above the earth) or geo-stationary satellites (36 000 km). Since Canada does not currently have any wireless communication capability using satellites, the CF rely on commercial and US military space assets. The data rates that are currently available vary between 2.4 Kbps to 256 Kbps. All communications carried over these networks are encrypted to ensure the security of the information being transmitted between network elements.

Over the next ten to fifteen years, commercial wireless systems will allow data rates of several Mbps. In terms of data communications, this would allow complete situational awareness to be transmitted to all personnel (this is not to say that all data will be available to all personnel). Link 22 is a tactical data link being developed to replace Link 11 (NATO Improved Link 11 – NILE). The objective is to enhance commanders' war-fighting capabilities by providing secure data links between network elements.

However, one field in wireless communications that should be explored is Ultra-Wide Bandwidth (UWB) technology. According to Multispectral Solutions, Inc. (MSSI), "the term 'ultra wideband' is a relatively new term to describe a technology, which had been known since the early 1960's as 'carrier-free', 'baseband', or 'impulse' technology. The basic concept is to develop, transmit and receive an extremely short duration burst of radio frequency (RF) energy – typically a few tens of picoseconds (trillionths of a second) to a few nanoseconds (billionths of a second) in duration. These bursts represent from one to only a few cycles of an RF carrier wave. The resultant waveforms are extremely broadband, so much so that it is often difficult to determine an actual RF center frequency – thus, the term 'carrier-free'. Early methods of signal generation utilized 'baseband' (i.e., non-RF), fast rise-time pulse excitation of a wideband microwave antenna to generate and radiate the antenna's effective 'impulse' response." [8].

Defence Relevance: In general, the research and development into wireless systems for military applications face the same challenges as in the past. These include security, availability, reliability and performance. "Since UWB waveforms are of such short time duration, they have some rather unique properties. In communications, for example, UWB pulses can be used to provide extremely high data rate performance in multi-user network applications. For radar applications, these same pulses can provide very fine range resolution and precision distance and/or positioning measurement capabilities. In fact, multifunction

architectures encompassing communications, radar and positioning applications have been developed." [9].

Annex S: Hyper-Spectral Sensing

Daniel Charlebois
DRDC ORD

Description: Spectral remote sensing has made huge strides in the last two decades regarding spatial and spectral resolution. There are currently sensors in space that have high spatial resolution (sub 0.5 m) as well as high spectral resolution (greater than 350 bands). These sensors are pushing terabytes of data down to earth on a daily basis. As computing power increases and new techniques are discovered in digital image analysis, we will be able to significantly increase the accuracy of surface attribute recognition. While discussing remote sensing, we must not neglect active sensors such as radar. More and more platforms are mounted with this type of equipment and the knowledge regarding radar image processing is increasing every day. Moreover the penetrating properties of radar allow us to view items that are not visible to spectral remote sensing devices.

Defence Relevance: Real time processing of remotely sensed data will provide much better situational awareness for both our allies and our adversaries.

Annex T: Chemical, Biological, Radiological Detection and Protection

Paul D'Agostino
DRDC Suffield

With contributions by Tom Cousins, DRDC Ottawa

"The most apparent trend is the probable significant proliferation of **biological weapons** with the number of states potentially possessing these more than doubling from four [China, Russia, North Korea, Iraq] to ten [India, Pakistan, Israel, Iran, Libya, Syria]" [10]. "Biological weapons **will** proliferate further and **may** become more sophisticated after 2015 and tuneable with respect to duration, survivability, transmission, lethality, potential resistance to medical countermeasures, and target specificity. At the same time more effective countermeasures **will** become available in terms of detection, protection and treatment but there is likely to be a lag before such countermeasures are derived." [7]. "**Chemical weapons** are generally available to those that would seek them, including non-state actors, as is the capability to develop basic **radiological weapons.** The means of delivering these weapons will also proliferate further, with more countries gaining short-range ballistic missiles, and current owners developing longer-range ballistic or cruise missile capabilities, either indigenously or through missile technology proliferation. Asymmetric delivery mechanisms such as civilian aircraft, ships, or sleeper devices, will also be available." [10].

Field Portable Chemical Detection Device(s)

Description: Traditional chemical warfare agents and non-volatile chemical warfare agents that are not adequately detected at present will soon be detectable by new chemical detection device(s).

Defence Relevance: These devices will be able to detect (point or standoff) traditional chemical warfare agents at lower levels more quickly in 'real-time' and will be able to detect non-volatile chemical warfare agents at low levels in time to protect field personnel at risk.

Field Transportable Chemical Identification System

Description: Chemical identification is presently limited to compound class differentiation (e.g. a nerve agent) using field portable device(s). New systems will enable rapid identification of the increasing list of agents of concern (chemical warfare agents, toxic industrial chemicals, etc.).

Defence Relevance: Although hand-held detection/identification device(s) will not be available for the increasing list of agents of concern (chemical warfare agents, toxic industrial chemicals, etc.), a transportable identification system based on mass

spectrometry will enable the CF to detect and identify the increasing list of agents and provide them with timely, rapid, and provisional identification

Field Portable Biological Warfare (BW) Agent Detection System

Description: BW agent detection systems have been both improving and becoming smaller in size. A prototype battery-operated, hand-held, real-time biological agent detector now exists and will likely be commercially available soon.

Defence Relevance: Smaller reliable devices will become the equivalent of the Chemical Agent Monitor (CAM) in chemical agent detection. Further work will likely allow the device to shrink even further, perhaps to the point of individual detectors. Networking these together in real-time on the battlefield may well eliminate false positives and provide far better data.

Field Portable BW Identification Systems

Description: Prototype field identification systems (e.g. Polymerase Chain Reaction PCR) are being tested under field conditions but are not at the stage for routine military use.

Defence Relevance: Field identification system using different technologies will eventually allow 'near-real time' identification. Combining systems with different technologies may lead to the ability to get confirmed identification in the field.

Sensitive Equipment Decontaminant

Description: Development of formulation for decontamination of sensitive equipment such as optical sights, electronics, night goggles and personal equipment capable of addressing traditional Chemical-Biological Warfare Agents (CBWA), non-volatile Chemical Warfare Agents (CWA) and Toxic Industrial Chemicals (TIC).

Defence Relevance: It will soon be possible to decontaminate sensitive equipment (for which there currently is no procedure or formulation available) which will be effective in a short time period, be easily removed, be compatible with equipment items and effectively address a wide range of traditional and potential CBW agents and TICs.

Improved Equipment/Vehicle Decontaminant

Description: Availability of less corrosive, longer-lived decontaminant formulation(s) with emphasis on agent/thickener solvation, detoxification of traditional and non-volatile CBWA and TICs and reduced formulation requirement.

Defence relevance: Current formulations are overly aggressive, stoichiometric in reaction and have limited lifetimes after preparation. Modifications will improve

compatibility with items being decontaminated and will be useable for longer periods of time. Thickeners, non-volatile CBWA and TICs will be more effectively addressed.

Nerve Agent Medication

Description: A human recombinant butylcholinesterase has been developed by transfecting goats with the human gene, which is expressed in mammary cells. Goats so transfected synthesize and secrete human butylcholinesterase in their milk. The enzyme can be isolated and purified from the milk and as such becomes useful for injection into humans since it would theoretically not precipitate an immune response (anaphylaxsis, etc.). Butyrylcholinesterase circulates in the blood and acts as a binding/inactivation site for nerve agents on a stoichiometric 1:1 basis and therefore this enzyme acts as a scavenger, effectively removing molecules of nerve agent before they can reach critical sites in the autonomic nervous system.

Defence Relevance: The injection of the enzyme could lead to a situation in which a human could be exposed to several LD_{50}'s of nerve agent and would show no signs of poisoning at all.[7] This would result in the first true prophylactic nerve agent treatment. Furthermore the enzyme has been produced and initial studies have proven the concept in animal experiments at DRDC and at the US Army's Institute of Chemical Defense (ICD).

Fieldable Hand-held Aerosol Inhaler Against BW Agents

Description: A new deployable, hand-held aerosol inhaler containing encapsulated ciprofloxacin which can be self-administered by a soldier in the field for protection against inhaled BW bacterial agents.

Defence Relevance: This new therapy can be effective against deadly inhaled BW agents such as inhalation anthrax and others, and it provides immediate protection and therapy in the field. No such medication exists at the present time.

Gene Expression as a Biological Marker of Radiation Exposure

Description: Radiation insult has been shown to cause vastly different end effects from one person to the next. Thus physical dosimetry may only be used as a 'guide' to biological consequences. The identification of specific expressed genes following radiation exposure is an ongoing project at DRDC Ottawa.

Defence Relevance: A field kit capable of analyzing samples (saliva, blood, etc.) from potentially exposed individuals will allow rapid triage and subsequent treatment based upon their individual response rather than that of an assigned dosimeter.

---

[7] LD_{50} is the dose (D) of liquid or solid nerve agent that is lethal (L) to fifty percent of the subjects exposed to it (i.e. the median lethal dose).

Field Remediation

Description: Current (national and international) regulatory limits demand so-called 'thorough' radiological decontamination of equipment and civilian infrastructure. A product of a current CBRN Research & Technology Initiative (CRTI) project will develop this.

Defence Relevance: If there is no portable decontamination system:

- Expensive equipment (vehicles) will not be allowed transport back to Canada.
- The CF will not be able to exercise due diligence and clean up areas in war-torn nations in order to allow unfettered civilian access.

Radiation Prophylactics and Therapeutics

Description: Such polysaccharides as beta-glucans stimulate the immune system, while certain vitamins are capable of scavenging reactive oxygen species that are produced by radiation and thus may be used as prophylactics. Cytokines may be used post-exposure to activate specific immune mechanisms and thus combat deleterious effects of radiation.

Defence Relevance: For missions in which there is an increased risk of radiation exposure, prophylactics may be administered. For individuals exposed, administering of therapeutics in the field will significantly lessen their biological detriment.

Standoff Radiation Detection

Description: Radiation detectors that are able to locate (and to a limited extent quantify) the presence of sources from distances greater than the specific radioactive particle's range (in-air).

Defence Relevance: The CF will be able to detect radiation without themselves (or even their equipment) being irradiated. For example an airborne survey of an alpha-contaminated field is possible.

Optically Stimulated Luminescence

Description: Radiation-induced traps in any material surrounding the current or previous location of a source may be excited (by laser) and their visible decay products (photons) observed.

Defence Relevance: Such a system may be used to expand the range of the standoff system mentioned above, thereby giving more warning of potentially hazardous environments. In addition, previous source location identification has clear value in weapons inspection/verification missions.

Networked Total Radiation Dosimetry Systems

Description: All current personal dosimeters yield accurate results only for gamma rays. Alpha, beta and neutron components are at best only inferred, and at worst ignored. Current R&D is aimed at an electronic personal dosimeter based on scintillating fibres. Future studies with thin membrane devices will address alpha and beta. Future dosimeters will have the capability to remotely broadcast the immediate dose rates, total dose to wearer and global positioning system (GPS) coordinates to any remote location in near real-time. Miniaturization of dosimetry and communications electronics will enable this.

Defence Relevance: On current missions the CF use traditional dosimeters, and thus will register as below for the fields from likely terrorist/military sources:

- PuBe – only about 10 % of dose (rest is neutrons);
- ^{90}Sr – only a few percent as all emissions are beta; and
- Pu – no dose registered, as all emissions are alpha and very low energy photon.

The networked "total" dosimeter would rectify these deficiencies. The commander (either on-scene or at home) will have an indication of the ongoing (i.e. Radiation Exposure Status RES) status of personnel, the immediate field dose-rate pattern and its previous temporal evolution. Thus much more timely decisions can be made.

Personnel Location by Radioactive Signature

Description: Personnel location and identification (via through wall sensing, etc.) is a definite need. All individuals have radioactive signatures, albeit at a low level. The problem of measuring the signal is strictly signal-to-noise. As techniques improve, (especially with so-called gamma ray telescopes) the measurement and location of concealed personnel becomes achievable.

Defence Relevance: Such a system is totally passive in nature and would be fairly compact, allowing ease of use.

Annex U: Autonomous Intelligent Systems

Doug Hanna
DRDC Suffield

Description: Autonomous Intelligent Systems (AIS) are individual systems or small teams capable of low complexity tasks in moderate complexity environments. They operate under human oversight along a sliding scale of autonomy that allows/requests operator input and/or direction for high complexity situations/decisions. Examples of roles and missions include: confuse opponents through diversionary operations; provide close reconnaissance support to manned reconnaissance operations; point vehicle in route reconnaissance; and autonomous multi-spectral, multi-agent detection and identification system for perimeter security role.

In an urban scenario, AIS could simultaneously invade urban buildings with heterogeneous multi-robot teams (10's-100's) from rooftops, from ground level, and from subterranean level. They could obtain a clear picture of how many personnel occupy the building, who they are and where they are located. Then troops could advance with the aid of superior situational awareness, assisted by robotic systems maintaining real-time picture of building and occupant status. The widespread use of AIS depends on solutions being found for compact high-energy sources.

Uninhabited Air Vehicles (UAV) will have AIS that can emulate a skilful pilot in tasks such as take-off, navigation, situation awareness, target identification, and safe return landing. Strategic and firing decisions will still require human intervention.

Defence Relevance: AIS can perform the dirty and/or dangerous and/or dull tasks while keeping higher value human assets out of harm's way. The United States will have this technology. Adversaries will not have access to it. AIS will mature and proliferate due to Western intolerance to casualties. AIS will be subject to rules of engagement.

Annex V: Non-Lethal Weapons

Pierre Lavoie
DRDC Ottawa

"True non-lethal weapons are discriminate weapons that are explicitly designed and employed so as to incapacitate personnel or material, whilst minimizing fatalities, and undesired damage to property and environment. Unlike weapons that permanently destroy targets through blast or fragmentation, many non-lethal weapons have (relatively) reversible effects on people. Developments are likely in acoustic, sonic, laser and microwave weapons, although whether such developments will still permit a genuine 'non-lethal' tag to be applied to weapons that incorporate such technologies is questionable. There is some concern that the 'non-lethal' nature of these weapons might tempt politicians, in some nations to task military forces to use them directly against civilian targets, particularly in public order situations, or lead to demands that they are used in preference to lethal weapons." [7].

High Power Microwave Weapon (HPM)

Description: Transportable high power microwave equipment that directs a beam of low frequency (a few GHz) microwaves to disrupt or destroy electronic devices (computers, sensors, navigation aids, communication devices) at a distance of hundreds of metres. Limitations are the large size, weight, power, relatively short weapon range, and that the aperture must be wide enough (e.g. 0.1 square meter) to prevent 30kV/cm air breakdown. Already, allies have demonstrated stopping of boats and cars.

Defence Relevance: The HPM weapon takes away the decision to use deadly force. Some allies will likely have some form of this technology. The CF can probably afford it. The vehicle stopping capability would help force and harbour protection against suicide bombers. The logistic support is simple as the HPM weapon runs off fuel or electricity.

Crowd Control High Power Microwave Weapon

Description: High frequency (90 GHz), smaller version of High Power Microwave weapon that transmits a beam of microwaves tuned to induce intense pain in the skin. Limitations are the size (e.g. 1 cubic meter), short range, and microwave absorption in rain. Allies have demonstrated such devices.

Defence Relevance: This technology can control crowds and maintain suspect individuals at a distance. The CF and allies will possibly have some form of it. Its likely uses include force and harbour protection against suicide bombers.

Electromagnetic Bomb (E-Bomb)

Description: "High power Electromagnetic (EM) Pulse generation techniques and High Power Microwave technology has matured to the point where (non-nuclear) E-Bombs are becoming technically feasible. The reliance of both the civil and defence sectors on electronics embedded in computers or communications equipment increases their vulnerability to EM attack. Currently the US and China are the only two nations with the established technology base to develop weapon systems based on this technology." [7].

Defence Relevance: The relative simplicity of the technology suggests that any nation or transnational network with even a 1940s technology base could have the capability to manufacture them. E-bombs offer high pay off with a modest commitment of resources and without the politically damaging loss of life [7]. The CF will need to protect their equipment against E-bombs.

Annex W: Ubiquitous Modelling and Simulation

Mark Hazen
DRDC Atlantic

Description: The term ubiquitous Modelling and Simulation (M&S) is almost as much a non-term as Network Centric Warfare. In its non-computer based forms M&S is always around us and used in everything we do. Hosted on computers (models, being algorithms or descriptions of processes and things) and simulations (being the application of models over time) are becoming more and more ubiquitous but not monolithic. The idea that one single simulation can cover all applications is a concept that comes primarily from people who do not develop simulations themselves or are far removed from the users. It has a certain amount of appeal in that theoretically a user learns one simulation and the procurement people only have to buy one simulation. However, the complexity of such a simulation is such that no individual user can become expert in all parts, just as in real life we have areas of specialty. The simulation requirements are just too diverse. No matter how much time you spend building a simulation, the next task after completing it will require something that was not included in it.

Therefore, task specific simulations are required and you need to drill down at least a layer of conceptual thinking. For example, you can go down a layer to say we want to develop simulation modules or tools to support acquisition (SEBA - Synthetic Environment Based Acquisition), or tactical development, or training, or R&D. Some of the components of these models will be usable by several areas and it is a good thing to design so that they can be. However, the detail level required to support tactical development is often very different from that required to support R&D of physical processes - and the issue of scaling fidelity levels is not at all simple. This does not mean that applications for concept development, might not be useful for developing tactics after a capability is acquired. However, it is more likely that the application will need to be modified (software or inputs) to match the actual capability from that envisioned in the concept development stage.

M&S as a tool consists not only of software, but also of the simulation inputs (system parameters, environmental parameters, module options, configuration files, etc.). In many simulations, changes in the inputs can change a simulation's fidelity level dramatically. It is the entire tool that must be verified and validated for each particular use. Processes for doing Verification, Validation and Accreditation (VV&A) are currently under development and review in the US and Canada. Verification compares a simulation (code and inputs) with a software specification - is it built right? Validation compares the specification with the user requirements and simulation outputs with reality- did we build the right thing? Accreditation is the user saying that the simulation meets their requirements. In a very few cases a simulation might be blanket accredited for use in applications with heavy caveats, and even then the user makes an accreditation decision to trust another opinion.

Defence Relevance: The military client needs assistance in a number of areas:

1. Provision of physical models of varying fidelity levels;

2. Provision of quality inputs to configure models;
3. Assistance in accreditation of simulations
    a. real data (with confidence limits) to validate simulations against
    b. conduct of sensitivity analysis of simulations to determine their areas of validity;
4. Expert advice on fidelity level required in simulations for various military applications;
5. Understanding how and when to link models of differing fidelities together; and
6. Provision of application specific simulations to support requirements.

Transformational Technologies

Annex X: Directed Energy Systems and Platforms

Dennis Nandlall
DRDC Valcartier

As a result of intensive research in physics, mechanical sciences, material science, chemistry and electronics, the future (the next 10 to 15 years) promises dramatic changes in military capability because of the significant impact these sciences will have on directed energy weapon systems and platforms. The following are some of the major technologies that could contribute to and significantly affect any Force Transformation process.

Heterogeneous Structural Systems Technologies

Description: Damage initiation and progression, failure mechanisms and life prediction were identified as essential for the development of new heterogeneous structural systems and, as a result, research in these areas has been ongoing for some time. "The mechanics of heterogeneous structures involves the development of integrated analytical, computational and experimental approaches to investigate the response of hybrid structures that may include combinations of high strength and lightweight engineered composites, ceramics and functionally graded materials. ... Physically based structural design guidelines for energy absorbing structural systems comprised of tailored combinations of materials and heterogeneities at different length and time scales," are currently being investigated. [11, p. 37].

Defence Relevance: There are technology barriers that are currently being investigated and need to be overcome if reliable structures such as helicopters, ground vehicles and weapon systems are to be designed, manufactured and maintained over a long period of time. From a materials standpoint there is a lot of work going on in the development of heterogeneous system and as a result these technologies will most certainly play a significant role in Transformation.

Adaptive Structures

Description: Adaptive structures, which include smart structures, structural dynamics, structural damping, active structural control, structural health monitoring, and inflatable structures are starting to gather attention mainly because of military requirements to become lighter and more mobile. Structures that can perform multiple functions are especially attractive from a protection viewpoint. From a materials/solid mechanics standpoint there is significant work currently being performed in advanced research and development of these systems. [11, p. 38]

Defence Relevance: These technologies are currently being considered for the next generation of missiles, projectiles, and weapon systems that will be used on the battlefield of 10 to 15 years.

Combustion and Propulsion

Description: The combustion and propulsion area literature seems to suggest that for missile and gun launch systems there are novel technologies in combustion processes that are emerging and that there is a high probability that they will be available in the next ten to fifteen years. Technologies such as plasma and laser induced ignition systems and thermal pyrolysis of basic ingredients of energetic materials and solid propellants will significantly affect the way weapons systems will be used in conflict situations. As a result, willing or not, Force Transformation will have to consider these newer technologies especially since lethality and precision can be significantly improved. [11, p. 41]

Electrical launch platforms

If this technology becomes available it will seriously affect any army transformation process, mainly because of the quantum leap that would be obtained in launch platforms. Literature has shown that significant accomplishments have been achieved over the past decade or so and it seems that electrical launch is now an inevitable technology. However, the question of when is not quite clear. Many of the fundamental hurdles have succumbed to a focussed, persistent combination of theory, analyses, computations and clever experiments. Today, instead of launching a few grams of plastic cubes, the capability of launching sophisticated integrated launch packages consisting of light weight armatures, long rod penetrators and low parasitic weight sabots now exists in the laboratory. In rail guns, carefully designed materials to prevent gouging, wear and erosion are replacing copper rails. In coil guns, large structures are capable of being accelerated with control and reliability not achievable with conventional chemical systems. In electro-thermo-chemical guns high temperature plasma ignition provides for propellant temperature compensation and reproducible propellant ignition. Power supplies have been reduced in size and mass from rotating machine and capacitor systems requiring large buildings to house them, to compact systems capable of being integrated into mobile tactical combat vehicles.

Defence Relevance: These technologies are still at the laboratory level and like other technologies still require significant effort for advanced technology demonstrators. Literature has shown clearly that electromagnetic launch technology has advanced so that practical applications are now inevitable in the 10 to 15 year time frame.

Advanced Kinetic Energy Penetrators

Description: Within the last decade, many ballistic researchers have investigated novel or unconventional kinetic energy penetrator concepts. Among them, segmented

and telescopic projectiles have had the greatest attention. Before hitting the target, a segmented projectile consists of a number of separated segments, while a telescopic projectile is composed of a leading core and a lagging tube. At velocities above 2.0 km/s it has been shown that both these unconventional projectiles give larger penetration in rolled homogeneous armour steel than a homogeneous projectile with the same initial geometry.

Reactive plasma phenomena technology

Literature has shown that this area in atomic, molecular and optical physics will offer fundamental changes and will influence the way direct energy weapon systems and platforms will evolve in the next 10 to 15 years. This area is creating fundamentally new capabilities for the military as well as providing the scientific underpinnings to enhance existing technologies. Advanced research has shown that "[l]ow temperature, reactive plasmas have demonstrated significant promise for solving several pressing Army needs: improved chemical warfare agent destruction; the reduction of emissions from diesel engines and flue gases; clean-up of soil contaminated with toxic chemicals; ignition and combustion control of gun propellants; and novel and high performance material science. In spite of the significant promise of plasma technologies, the design, optimization, and implementation of these technologies has been greatly impeded by the lack of a detailed understanding of the plasma chemical, electrical and physical processes" that is needed for design and optimization. [12].

Mobile Tactical High-Energy Laser (MTHEL)

"Weapons that travel far faster than the proverbial speeding bullet are as little as five years from use in combat, say defense officials who used a laser to shoot an artillery shell out of the sky … The so-called Mobile Tactical High-Energy Laser is a short-range weapon being co-developed with Israel, which wants it to destroy Katyusha rockets fired at its border villages by Hezbollah guerillas in Lebanon. The chemically powered weapon, which looks like a searchlight, is one of a handful of laser devices the Pentagon is working on under the umbrella of missile defense." [13].

"A study completed in 2001 concluded that the rocket interceptor has 'lots of promise' and further development should be pursued, primarily in enabling system's mobility. Mobility considerations for the future mobile systems include system mobility (road and off road capabilities) and air transportability, including the type of transport aircraft it should fit on (C-130, C-17 or C-5). Conclusions of these studies will define the necessary size-reduction technologies required for the future version. Further studies of the system include the use of such laser beam weapons to provide 'hard kill' defenses against artillery projectiles, UAVs and cruise missiles." [14].

Defence Relevance: Most of the work done on novel types of penetrators involved very small-scale projectiles. Recently there is some effort on the development of prototypes and this signals the integration of these types of projectiles in the next ten years. This type of technology combined with advanced launching techniques will certainly have significant effect on any Force Transformation.

Advanced state-of-the art research in experimentation and modelling and simulation is under way to develop plasma reactors tailored for defence applications in the near future

Development of the Mobile Tactical High Energy Laser weapon is expected to accelerate as the US Army is concluding studies to build the mobile version of the anti-rocket system. The US Army budgeted US $118 million for the program from 2003 to 2007. [15].

Thermobaric Round

Description: "The thermobaric round combines the current … airburst capability with thermobaric ammunition that utilizes a single initiation with a two-staged event – the dispersal of an explosive mixture into the air followed by ignition. After the thermobaric cartridge impacts the target, the initial explosion disperses fine thermobaric explosive particles into the air and auto-ignites, which creates an overpressure." [16].

Defence Relevance: "The resulting particle cloud formed by thermobaric ammunition fills the entire lethal area, potentially resulting in 100 percent probability of hit in targets, such as buildings and caves …[It provides] soldiers with a decisive overmatch capability by increasing lethality, range and capability." [16].

Annex Y: Cyber-War Technologies

Daniel Charlebois
DRDC ORD

Strong Encryption

Description: "The demand for **encryption** on information systems will increase, driven by the complementary needs of privacy, security and financial transactions. Strong encryption and authentication procedures, developed by commercial specialist firms, will become more widespread. Before 2015 unbreakable encryption (e.g. using quantum cryptography) could be available. … Given that market demands will drive security issues and that IT expertise is likely to spread beyond US dominance, it is judged that strong commercial encryption technologies are likely to be widely available outside the control of governments." [7].

Of significant concern is that the US military has planned to replace all cryptographic equipment within the next 10-15 years. As a result, the CF will be compelled to upgrade their own equipment to ensure that interoperability with the US forces is not an issue during our participation in combined deployments.

Defence Relevance: "The diffusion of commercially available strong encryption is **likely** to mean that the privacy and surveillance arena becomes more contested, potentially reducing the US-UK advantage in strategic signals intelligence." [7].

Quantum Computers

Description: "[I]n 1994 … Peter Shor from AT&T's Bell Laboratories in New Jersey devised the first quantum algorithm that, in principle, can perform efficient factorization. This became a `killer application' – something very useful that only a quantum computer could do. Difficulty of factorisation underpins security of many common methods of encryption; for example, RSA – the most popular public key cryptosystem which is often used to protect electronic bank accounts gets its security from the difficulty of factoring large numbers. Potential use of quantum computation for code-breaking purposes has raised an obvious question – what about building a quantum computer.

In principle we know how to build a quantum computer; we can start with simple quantum logic gates and try to integrate them together into quantum circuits. A quantum logic gate, like a classical gate, is a very simple computing device that performs one elementary quantum operation, usually on two qubits, in a given period of time. Of course, quantum logic gates are different from their classical counterparts because they can create and perform operations on quantum superpositions. However if we keep on putting quantum gates together into circuits we will quickly run into some serious practical problems. The more interacting qubits are involved the harder

it tends to be to engineer the interaction that would display the quantum interference. Apart from the technical difficulties of working at single-atom and single-photon scales, one of the most important problems is that of preventing the surrounding environment from being affected by the interactions that generate quantum superpositions." [17].

Defence Relevance: Operations on quantum superpositions are the holy grail of code breaking. The US will lead the planet on this front and for national security reasons will not disclose this technology, even with its allies. The capacity of the US to break codes will far exceed that of any other country.

Global Information Network

Description: As information systems and networks penetrate the global environment, we are witnessing the proliferation of ease of access to information into all corners of the globe. Although it will provide many benefits to all societies, it also offers many opportunities to our adversaries to discover valuable information regarding our national security. Every new network element, protocol, firewall, etc. provides a means of breaking in and thus makes us vulnerable. Also, our reliance on these systems makes us vulnerable to misinformation, identity theft, denial of service, etc.

Defence Relevance: Critical systems will be part of this network and subject to attack, identity theft, misinformation and other forms of attacks that can have a significant impact on the success of allied operations.

Annex Z: New Materials

Dennis Nandlall
DRDC Valcartier

Description: To a large extent, for the latter half of the solid-state based 20th century it seems that materials science has been the engine that propelled technology. Within recent years, with the demand for lighter weight and higher performance systems for future armed forces, it has been recognized that emphasis in material programs has increasingly shifted away from metals research to programs that cover a broad spectrum of materials including polymers, ceramics and semi-conductor materials. Because of this growing insatiable demand for new materials for emerging technologies, it seems abundantly clear that current trends in materials science now at the beginning of the 21st century will have profound effects on the Transformation of future armed forces. Research trends seem to focus on the development of new materials; material processes and properties that promise to significantly improve performance, increase reliability and reduce cost of future military systems. Review of literature seems to indicate that polymer-based materials have already been associated with important sectors of industry both in production as well as in application. Further growth is strongly expected due to anticipated availability of smart materials and technologies in the near future.

The following are current basic material research trends that will most likely play an important role in shaping the development of materials within the next 10 to 15 years. From a military standpoint it seems natural they will certainly have an important impact on any Force Transformation process.

- Synthesis and processing of materials;
- Physical behaviour of materials;
- Mechanical behaviour of materials;
- Materials reliability;
- Advanced solid mechanics;
- Hierarchical and smart materials;
- Bio-molecular and cellular materials and processes;
- Design and control of smart and adaptive structures;
- Photonic band gap materials; and
- Solid-state devices – electro, magnetic and optical materials.

Defence Relevance: As shown in the Figure below, it seems that these technologies will be critical drivers of innovation in advanced technologies, devices and systems that in the near future will bring the benefits of sustainable development and competitiveness to sectors such as transport, energy, medicine and health care, electronics and construction. These are the sectors that will affect and, willingly or not, influence the military Transformation.

Figure 2. Defence related areas that could be influenced in the next 10 to 15 years by material technology research areas

Future Logistics

Pump Converting Vehicle Exhaust into Water

Description: A "pump combines oxygen and hydrogen in vehicle exhaust into water. The water comes about by taking the hydrogen, which is also already present in the fuel, and combining it with oxygen… That oxidation makes water… The process involves regenerative heat exchangers, evaporative coolers, filters and pumps. The vehicle exhaust moves from the

exhaust system to a heat exchanger. That exchanger lowers the temperature of the exhaust before it hits those coolers. The cooler is similar to a car's Freon-based air conditioner… The cooler lowers the exhaust temperature to a point where water starts to condense… For every two gallons of fuel, the pump can make about one gallon of water. In other words, if a Humvee's fuel tank is 30 gallons, the system can produce about 15 gallons of drinkable water." "[T]he pumps when fielded may cost about $25,000 each." [18].

Defence Relevance: A soldier's drinking water requirement is anywhere from three to four gallons per day. Currently the U.S. Army is using 40 percent of its supply chain on distributing water in Iraq. By minimizing the amount of water being sent forward, this technology will reduce demand and burden on the logistical tail. [18]

Annex AA: Cognitive Sciences

Justin Hollands
DRDC Toronto

With contributions by Jocelyn Keillor, DRDC Toronto

Description: The notion of implanting devices in the brain to improve human capacity is still very much science fiction. However, some studies have been conducted that suggest that brain activity can be influenced in a gross way by electromagnetic stimulation or chemical treatment.

One may distinguish between implantable and peripheral devices (Garcia-Rill [19]), and we are probably closer to fruition with the peripheral devices.

The technique of transcranial magnetic stimulation (TMS) has been refined in recent years to allow the delivery of a train of 2-tesla, 1 ms magnetic pulses at about 1 Hz. This technology is called repetitive TMS (rTMS), and disrupts brain activity for tens of minutes, creating 'virtual lesions' that affect performance. Most of the time, rTMS has negative effects, producing a kind of random neural noise, but in at least one documented case, Boroojerdi et al., [20], enhanced performance has been produced. In this study, the researchers applied rTMS to the prefrontal cortex of participants solving a spatial reasoning puzzle, and the time taken to solve the problem was reduced with the rTMS stimulation relative to sham control and a condition where another brain region was stimulated. This contrary result might be due to a kind of stochastic resonance effect (addition of noise inducing state change). However, whether something that works by disrupting established neural patterns has a high potential for improving overall performance in the field is unknown. The rTMS device appears to be approximately 15 cm x 15 cm x 5 cm with a transmitting cable and requires stationary head position (see pictures in [21]). If rTMS technology could be miniaturized to produce a smaller and lighter peripheral device, or could be implantable (perhaps at nanotechnology scale), there may be potential to improve human performance in operational settings.

The Neural Engineering Laboratory in the Department of Biomedical Engineering at the University of Michigan is involved in a multi-institutional project to develop cortical implant systems for use in humans. The work is described on a secure website.[8] They are examining active delivery of chemical and biological agents in real time using flow controllers operating with a feedback control loop. There are issues with glial cell build up on probes—this build up stops probes from operating accurately over time. Further, there are problems with micromotion of the probe. Active delivery of chemical and biological agents in real time is available using flow controllers operating with a feedback control loop.

Researchers at Wayne State University (Ligon Research Center of Vision) are investigating cortical implants with respect to the visual system. A cortical implant would receive visual signals from an external, electronic sensor, and then process them into information that the

[8] See http://nelab.engin.umich.edu/Global/Content.aspx?ModMenuID=6

cortex could translate into a recognizable picture."[9] They indicate that brain plasticity presents a problem.

Some argue that a person's appraisal of a feature of the environment as stressful is more important than the objective characteristic of the threat [19, 22]. This has led to an interest in reducing distractibility (essentially a lack of focussed attention) or monitoring its level. Sensory gating (filtering out extraneous information) may be assessed by the P50 potential, a midlatency auditory evoked potential. Garcia-Rill argues for the development of a nanoscale module designed for the use of the P50 potential as a measure of sensory gating. The module would include an electronically shielded helmet with P50 potential recording electrodes at vertex, mastoids and ground, eye movement recording using flip-down transparent screen (one eye), electrodes on forehead to monitor potentially interfering forehead muscle contractions.

Garcia-Rill also discusses measurement of hypofrontality (decreased blood flow to the frontal cortex), which leads to instinctive, exaggerated fight *vs* flight behaviour. Since hemoglobin is a strong absorber, changes can be monitored using near-infrared detection.

Finally, brain imaging technology has made significant strides in the last 5-10 years, with fMRI's (functional magnetic resonance imaging) and PET (positron emission tomography) as the leading technologies. fMRI's have a resolution limit of about a cubic millimeter, this volume can still contain tens of thousands of neurons. PET scans are more accurate in determining where in the brain neurons are being activated but have poorer temporal resolution. Countless studies have been establishing what brain regions are involved when people perform specific types of tasks. This knowledge should feed forward into the design of cortical implants and cognitive technologies more generally.

DARPA has a Brain Machine Interface Program, which seeks to develop new technologies for augmenting human performance by accessing the brain in real time and integrating the information into external devices [23]. Funding from this program helped create the Duke University Center for Neuroengineering, where Miguel Nicolelis' research in brain machine interfaces has been recognized in MIT's *Magazine of Innovation Technology* as among the top ten "Emerging Technologies That Will Change the World." [24].

In terms of implantable devices, using nanotechnologies to monitor and modulate neurochemical or hormonal levels appears feasible but has not yet been demonstrated.

Defence Relevance: "Recent advances in the fabrication and implantation of wireless interfaces in the brain have successfully translated motor and sensory commands into controlling peripheral devices such as robotic arms. It is also likely that human-machine interface technologies such as sophisticated visualisation technologies (e.g. virtual reality), wearable devices and pervasive computing will mature, easing interaction and potentially reducing the skill levels necessary to operate typical ICT [Information and Communications Technology] technology. It is not clear whether society is ready to accept such invasive systems. Many may view such developments as an infringement of civil rights and will

[9] See Mertz, L. Let There be Sight. (Online). Wayne State University. http://www.med.wayne.edu/Wayne%20Medicine/wm2000/lettherebesight.htm (4 Feb. 2004).

continue to prefer systems with a human input but which are user-friendlier. Certainly such developments will provoke strong legal, moral and ethical debate." [7].

Annex BB - Terms of Reference - Defence R&D Canada (DRDC) Tiger Team on Transformation Concepts

Role of the Tiger Team

The DRDC Tiger Team on Transformation provides information, analysis and advice to members of Research and Development Executive Committee (RDEC) concerning military and departmental Transformation Concepts and their implications for DRDC. The Tiger Team will:

- Provide information and analysis of the attributes of Transformation and describe relevant military Transformative concepts – including the issues surrounding potentially disruptive technology innovations;
- Advise on the positioning of the Agency's R&D program with respect to DND/CF Transformation, long-term strategic objectives, the Force Development process and long-term capability/equipment targets; and
- Provide a forum for a discussion of Transformation issues of mutual concern and interest to participants and stakeholders.

Output of the Tiger Team

The Tiger Team will produce a written Report that contains information, analysis and recommendations to be submitted to the RDEC for their consideration in setting priorities and making decisions with respect to the role of DRDC in Transformation.

Annex CC - Terms of Reference - Defence R&D Canada (DRDC) Tiger Team on Technologies for Transformation

Role of the Tiger Team

The DRDC Tiger Team on Technologies for Transformation provides information, analysis and advice to members of Research and Development Executive Committee (RDEC) concerning militarily relevant technologies that will affect defence and security in the Canadian context. The Tiger Team will:

- Provide information and analysis of a wide variety of technologies that will be battlefield-ready within the next ten years;
- Provide information and analysis on potentially disruptive technologies (new or existing technologies used in an innovative fashion that significantly alter established practices) out to Horizon III;
- Advise on the positioning of the Agency's R&D program with respect to these technologies and their impact on the Force Development process and long-term capability/equipment targets; and
- Provide a forum for a discussion of advanced technology issues of mutual concern and interest to participants and stakeholders.

Output of the Tiger Team

The Tiger Team will produce a written Report that contains information, analysis and recommendations to be submitted to the RDEC for their consideration in setting priorities and making decisions with respect to the role of DRDC in bringing new technologies into service with the Canadian Forces.

Appendix A: Transformation Concepts Matrix

Jim Kennedy – DRDC Atlantic

Specific topics are raised with the Transformation Concepts essays and, frequently, the same topic arose in several of the essays. By identifying the common topics it is clear to see those that are pervasive, thereby appearing in almost all of the concepts. Topics that are pervasive are clearly of some importance to Transformation.

The extent to which DRDC is addressing identified topics gives some measure of how we are addressing Transformation. To aid in visualizing this, Table 3 provides an assessment of how much Technology Investment Strategy (TIS) activity is currently being put towards the topics, as they refer to each concept. The magnitude of the activity is colour coded in the three levels; no activity, some activity, and enough activity. The TIS numbers come from the original TIS and are listed in Table 2. Topics gleaned from the essays appear on the left side of Table 3 while the overall concepts addressed by the essays appear at the top of Table 3.

Table 2. Technology Investment Strategy

NO.	R&D ACTIVITY
3	Command and Control Information Systems Performance and Experimentation
8	Information and Knowledge Management
4	Communications
7	Human Factors Engineering and Decision Support Systems
14	Command Effectiveness and Behaviour
1	Autonomous Intelligent Systems
16	Sensing (Air and Surface)
17	Underwater Sensing and Countermeasures
20	Space Systems
5	Electro-Optical Warfare
15	Radio Frequency Electronic Warfare
10	Network Information Operations
13	Precision Weapons
21	Weapons Performance and Countermeasures
6	Emerging Materials and Biotechnology
18	Signature Management
12	Platform Performance and Life Cycle Management
9	Multi-Environment Life Support Technologies
11	Operational Medicine
2	Chemical/Biological/Radiological Hazard Assessment, Identification and Protection
19	Simulation and Modelling for Acquisition, Requirements, Rehearsal and Training
22	Operational Research

Table 3. Transformation Concepts Matrix

Topics		Transformation Concepts																										
		Human factors																										
Clumps	*Detail*	Predictions	Preamble	Knowledge use	Cultural translation	SMARRT	Enhanced Performance	Network Centric Warfare	Interoperability	Non-invasive personnel ID	Autonomous Systems	Effects Based Planning	Network / Information Protection	Full Spectrum Protection	Integrated ISR	Technological Red Team	Knowledge / Experience Capture	Process Improvement	Footprint Reduction	Capability-Based Force Development								
Computers	Quantum																											
	Machine learning										17																	
	Reliability & protection								10				10		10		10	10										
Systems	Responsive	many									1			6														
	Flexible										many							19										
Threat detection	Remote									16?	18,20			16,17 ,20														
	Concealed										18			16,17 ,20														
Enhanced soldier	Physical							9																				
	Mental & intellectual		7	7																								
	Adaptable	7?										7?					7?											
Protected soldier	Physical													9														
	Emotional well-being																											
Culture	Understand others																											
	Trust			7			7	14	14			14					14											
	Handle uncertainty														14													
	Training	14?				19											14?											
Net enabled	Data fusion & extraction			17				17						17,8			17											
	Information sharing							10,8			1						8			8								
	Netcentricity										10																	
Joint & combined	Coordination											15?																
	Inter-operability					19			17			15	10															
Operational planning	Planning tools										22							22										
	Scenarios & testing					12						22				22												
	Outcomes & expectations										22?								22									
Speed	Mobility									12																		
	Rapid response																											
Others	Urban environment										16																	
	Value & efficiency		many			12					many							many	many									
	New materials													6														
	Distributed infrastructure												10															
	Portable power													6					6									
	Symbols	DRDC activity			None				Some				Enough				Numbers denote TIS activity											

References

1. Much of what follows is taken directly from Fewell, M.P. and Hazen, M.G. (2003). Network-Centric Warfare—Its Nature and Modelling. (DSTO-RR-0262). (Online) Defence Science and Technology Organisation. http://www.dsto.defence.gov.au/corporate/reports/DSTO-RR-0262.pdf (4 Feb. 2004).

2. Network Centric Warfare. (Online) Department of Defense Report to Congress, 27 July 2001. http://www.dodccrp.org/research/ncw/ncw.htm (1 Mar. 2004). Another version of the tenets can be found in Alberts, D.S. (2002). Information Age Transformation: Getting to a 21st Century Military. Revised. (Online) Washington, D.C.: CCRP Publication Series, pp. 7-8. http://www.dodccrp.org/research/ncw/ncw.htm (1 Mar. 2004). For a criticism of the NCW thesis and these tenets see Giffin, R.E. and Reid, D.J. (2003). A Woven Web of Guesses, Canto Two: Network Centric Warfare and the Myth of Inductivism. (Online) Presentation to 8th International Command & Control Research & Technology Symposium, National Defense University, p 6. http://www.dodccrp.org/events/2003/8th_ICCRTS/Pres/track_5.htm (1 Mar. 2004).

3. See Garstka, J. and Pattillo, C. (2003). A Conceptual Framework for Network Centric Operations. (Online) Presentation to Network Centric Warfare Conference, Brussels, Belgium. http://www.oft.osd.mil/library/library.cfm?libcol=2 (4 Feb. 2004). For a recent example of this framework see Holloman, K. (2003). Network Centric Operations Conceptual Framework. (Online) Presentation to Center for Research on Information Technology and Organizations, California, USA. http://www.oft.osd.mil/library/library.cfm?libcol=2 (4 Feb. 2004).

4. Salmanian, M. (2003). Military Wireless Network Information Operation Scenarios (DRDC Ottawa TM 2003-241). (Online) Defence R&D Canada - Ottawa. http://cradpdf.drdc-rddc.gc.ca/PDFS/unc17/p520923.pdf (27 Apr. 2004).

5. The contents of this section are edited from Lefebvre, J.H., Grégoire, M., Beaudoin, L., and Treurniet, J. (2003). Joint Network Defence and Management System: Concept Document Technical Report. (DRDC Ottawa TM 2003-230). Defence R&D Canada - Ottawa.

6. Fulghum, D.A. (2003). New Sensors to Iraq. *Aviation Week and Space Technology*, 159 (17), p. 26.

7. Strategic Trends. The Science and Technology Dimension. (Online) Joint Doctrine and Concepts Centre, UK Ministry of Defence. http://www.jdcc-strategictrends.org (8 Jan. 2004).

8. Multispectral Solutions, Inc. What is ultra wideband technology? (Online). http://www.multispectral.com/UWBFAQ.html (9 Dec. 2003).

9. Multispectral Solutions, Inc. What are the advantages of UWB technology? (Online). http://www.multispectral.com/UWBFAQ.html (9 Dec. 2003).

10. Strategic Trends. The Military Dimension. (Online). Joint Doctrine and Concepts Centre, UK Ministry of Defence. http://www.jdcc-strategictrends.org (8 Jan. 2004).

11. Army Research Laboratory. (2003). Broad Agency Announcement for Contracts, Grants, Cooperative Agreements, and Other Transactions. (Online) U.S. Department of Army. www.aro.army.mil/research/arl/fy06arlbaa.pdf (4 Feb. 2004).

12. Army Research Office. (2000). Physics – ARO in Review 2000. (Online). U.S. Department of Army. www.aro.army.mil/aronreview/physics00/physics00.htm (4 Feb. 2004).

13. Military Laser Nearly Ready for Combat. (Online) *Globe and Mail.* http://www.globeandmail.com/servlet/ArticleNews/front/RTGAM/20021111/gtlaser/Front/homeBN/breakingnews (8 Jan. 2004).

14. Tactical High Energy Laser (THEL) Program. (Online) *Defense Update.* http://www.defense-update.com/directory/THEL.htm (8 Jan. 2004).

15. Israel is expected to increase funding for Laser Weapon. (Online) *Defense Update.* http://www.defense-update.com/news/MTHEL.htm (8 Jan. 2004).

16. Daubert, J. (2003). First 25mm thermobaric airburst round fired from XM307 crew served weapon. (Online) U.S. Newswire. https://peosoldier.army.mil (21 Nov. 2003).

17. Barenco, A., Ekert, A., Sanpera, A. and Machiavello, C. (1996). L'ordinateur sous le charme quantique: Un saut d'échelle pour les calculateurs. *La Recherche,* No. 292. Nov. p. 52. Adapted by A. Barenco (Online) Centre for Quantum Computation. http://www.qubit.org/library/intros/comp/comp.html (8 Jan 2004).

18. Putnam, B. (2003). Army Testing Pump that Makes Water from Exhaust. (Online) Army News Service. http://www4.army.mil/ocpa/read.php?story_id_key=5311 (8 Jan. 2004).

19. Garcia-Rill, E. (2002). Focusing the possibilities of nanotechnology for cognitive evolution and human performance. In M. C. Roco and W. S. Bainbridge (Eds.), *Converging technologies for improving human performance,* pp. 227-232. Arlington, Virginia: National Science Foundation.

20. Boroojerdi et al. (2001). Enhancing analogic reasoning with rTMS over the left prefrontal cortex. *Neurology, 56,* pp. 526-528.

21. Chicurel, M. (2002). Neuroscience: Magnetic mind games. *Nature* [electronic journal] 417, no. 6885. pp. 114-116. URL: http://www.nature.com/cgi-taf/dynapage.taf?file=/nature/journal/v417/n6885/index.html

22. Committee on Space Biology and Medicine. (1998). A Strategy for Research in Space Biology and Medicine in the New Century. (Online) National Research Council. Washington, D.C.: National Academy Press. http://www.nap.edu/books/0309060478/html/index.html (6 Jan. 2004).

23. Duke University. (2002). DARPA To Support Brain-Machine Research (Online) Pratt Press. http://www.pratt.duke.edu/Newsletter/Issue9/story4.html (10 Feb. 2004). Eisenstadt, E. (2002). Brain Machine Interface. (Online) Defense Sciences Office. Presentation to DARPATech 2002 Symposium, Anaheim, California. http://www.darpa.mil/DARPATech2002/presentations/dso_pdf/speeches/EISENSTADT.pdf (10 Feb. 2004). Defense Sciences Office. Human Assisted Neural Devices. (Online) DARPA. http://www.darpa.mil/dso/thrust/biosci/brainmi.htm (10 Feb. 2004). Zimmer, C. (2004). Mind Over Machine. Popular Science [electronic journal] February 2004. URL: http://www.popsci.com/popsci/medicine/article/0,12543,576464-1,00.html .

24. Duke University. Duke Center for Neuroengineering. (Online) http://bme-www.egr.duke.edu/Research/Elecphys/Neuroeng/Neuro.htm (10 Feb. 2004).

List of symbols/abbreviations/acronyms/initialisms

AI	Artificial Intelligence
AIS	Autonomous Intelligent System
BW	Biological Warfare
C2IS	Command and Control Information System
CAM	Chemical Agent Monitor
CBR	Chemical, Biological, Radiological
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CBWA	Chemical-Biological Warfare Agent
CF	Canadian Forces
CFNOC	Canadian Forces Network Operations Centre
COA	Courses of Action
CRTI	CBRN Research & Technology Initiative
CSA	Canadian Space Agency
CWA	Chemical Warfare Agent
DGRDP	Director General Research and Development Programs
DND	Department of National Defence
DRDC	Defence Research and Development Canada
DST Pol	Directorate Science and Technology Policy
EO	Electro-Optical
EBO/P	Effects Based Operations/Planning
EM	Electromagnetic
FMRI	Functional Magnetic Resonance Imaging
GIS	Geographic Information System

GMTI	Ground Moving Target Indicator
GPS	Global Positioning System
HPM	High-Power Microwave
HVAC	Heating, Ventilating, and Air Conditioning
ICD	Institute of Chemical Defense
ICT	Information and Communications Technology
ISR	Intelligence, Surveillance, Reconnaissance
IT	Information Technology
JNDMS	Joint Network Defence and Management System
M&S	Modelling and Simulation
MSSI	Multispectral Solutions, Inc.
MTHEL	Mobile Tactical High-Energy Laser
NATO	North Atlantic Treaty Organization
NBC	Nuclear, Biological, Chemical
NCO	Network Centric Operations
NCW	Network Centric Warfare
NEC	Network Enabled Capability
NGO	Non-Governmental Organization
NILE	NATO Improved Link 11
NIO	Network Information Operations
NRC	National Research Council Canada
OGD	Other Government Department
ONA	Operational Net Assessment
ORD	Operational Research Division

PCR	Polymerase Chain Reaction
PET	Positron Emission Tomography
POL	Petrol, Oil, Lubricants
PRICIE	Personnel (including professional development and leadership); Research & Development/Operational Research; Infrastructure & Organization; Concepts, Doctrine and Collective Training; Information Technology Infrastructure; and Equipment, Supplies and Services.
R&D	Research and Development
RDEC	Research and Development Executive Committee
RES	Radiation Exposure Status
RF	Radio Frequency
SAR	Synthetic Aperture Radar
SEBA	Synthetic Environment Based Acquisition
SCM	Supply Chain Management
SIGINT	Signals Intelligence
SMARRT	Simulation and Modelling for Acquisition, Requirements, Rehearsal, and Training
SOC	Strategic Operating Concept
TAWG	Technology Assessment Working Group
TDP	Technology Demonstration Program
TIC	Toxic Industrial Chemical
TIS	Technology Investment Strategy
TMS	Transcranial Magnetic Stimulation
TSSU	Tactically Self-Sufficient Unit
UAV	Uninhabited Air Vehicle
UN	United Nations

UWB	Ultra-Wide Bandwith
VV&A	Verification, Validation and Accreditation
WMD	Weapons of Mass Destruction

DOCUMENT CONTROL DATA SHEET

1a. PERFORMING AGENCY	2. SECURITY CLASSIFICATION
Defence R&D Canada 305 Rideau Street Ottawa, Canada K1A 0K2	UNCLASSIFIED -
1b. PUBLISHING AGENCY Defence R&D Canada 305 Rideau Street Ottawa, Canada K1A 0K2	

3. TITLE

(U) Transformation Concepts and Technologies: DRDC Tiger Team analysis of Transformation implications

4. AUTHORS

Neal Porter, Jim Kennedy, Bert Bridgewater, et al.

5. DATE OF PUBLICATION	6. NO. OF PAGES
April 27 , 2004	96

7. DESCRIPTIVE NOTES

8. SPONSORING/MONITORING/CONTRACTING/TASKING AGENCY

Sponsoring Agency:

Monitoring Agency:

Contracting Agency :

Tasking Agency:

9. ORIGINATORS DOCUMENT NO.	10. CONTRACT GRANT AND/OR PROJECT NO.	11. OTHER DOCUMENT NOS.
Technical Report TR 2004-003	20a	CANDIS SYSNUM: 521343; DRDKIM Accession Number: CA023987

12. DOCUMENT RELEASABILITY

Unlimited distribution

13. DOCUMENT ANNOUNCEMENT

Unlimited announcement

14. ABSTRACT

(U) The Department of National Defence and the Canadian Forces are presently analysing the implications of Transformation and the future defence and security environment. Defence Research and Development Canada (DRDC) established two Tiger Teams in order to inform and enable that process. The teams conducted a workshop in October 2003 and then exchanged information through the use of a portal before consolidating their findings. One team analysed a variety of Transformation concepts and came to the conclusion that three influences pervaded all of the concepts. These were the issues of the role of culture, the soldier's capability, and being networked enabled. It was felt that DRDC was only very well positioned to support the latter. The other team examined technologies that would enable Transformation in the next 30 years. It determined that directed energy systems and platforms, cyber-war technologies, new materials, and cognitive sciences would be among the disruptive technologies in the future. These are new or existing technologies used in an innovative fashion that will significantly alter established practices. The teams' findings set the stage for further discussion of Transformation and the future science and technology environment.

(U) Le ministère de la Défense nationale et les Forces canadiennes sont en train d'analyser l'incidence de la transformation ainsi que le futur cadre de défense et de sécurité. Recherche et développement pour la défense Canada (RDDC) a constitué deux équipes spéciales chargées de la diffusion d'information et de la mise en oeuvre de ce processus. Avant de rassembler leurs constatations, elles ont tenu un atelier, en octobre 2003, puis échangé des renseignements grâce à l'utilisation d'un portail. Une équipe a analysé divers concepts de transformation et en est venue à la conclusion que trois facteurs déterminants se retrouvaient dans tous les concepts. Il s'agissait du rôle de la culture, de la capacité du soldat et de la possibilité de réseautage. On estimait que RDDC n'était en mesure d'appuyer que le dernier. L'autre équipe a examiné des technologies susceptibles de faciliter la transformation au cours des 30 prochaines années. Elle a déterminé que les systèmes et plates-formes à énergie dirigée, les technologies de cyberguerre, les nouveaux matériaux et les sciences cognitives feraient partie des technologies perturbatrices de l'avenir. Ce sont des technologies nouvelles ou existantes qui sont utilisées d'une manière innovatrice, de sorte qu'elles modifient considérablement les pratiques établies. Les conclusions des équipes ouvrent la voie à d'autres discussions sur la transformation et le futur cadre des sciences et de la technologie.

15. KEYWORDS, DESCRIPTORS or IDENTIFIERS

(U) Transformation; Future Environment; Disruptive Technology; Battlefield Ready Technology; Culture; Network Centric Warfare; Effects Based Operations